الجامعة اللبنانية

كلية الحقوق والعلوم السياسية والادارية

العمادة

حماية الخصوصية والبيانات الشخصية في القانون اللبناني والمقارن

رسالة معدة لنيل شهادة الماستر البحثي في القانون العام

اعداد: ليال بهنام

لجنة المناقشة:

الدكتور عصام اسماعيل	الاستاذ المشرف	رئيسا
الدكتور وسام غياض	استاذ	عضوا
الدكتور جوزيف رزق الله	استاذ مساعد	عضوا

٢٠٢٠



الجامعة اللبنانية غير مسؤولة عن الآراء الواردة في هذا البحث، وهي تعبر عن رأي صاحبها فقط.

الاهداء

الى ابنتي، التي دعمت عودتي الى مقاعد الدراسة وتحملت كثرة انشغالي وغيابي وعملي على هذا البحث في اوقات العطل التي كنت اخصصها لها. على امل ان اكون قد نقلت لها ان قيمتنا كنساء في ما ننتج من علم وما نرفد فيه النقاشات العامة بغية ان يكون دورنا فاعلا في مجتمع يؤمن مساحة متساوية للجميع.

الى مؤسسة مهارات ومديرتها رلى مخايل، التي تعلمت منها الكثير وساهمت في تشكيل فكري النقدي ووسعت آفاقي العلمية وأمنت لي كل الدعم لاكمل مسيرتي البحثية، على ان يشكل هذا البحث موردا اضافيا لمكتبة هذه المؤسسة التي اصبحت مرجعا في الحريات العامة.

الشكر والتقدير

الى استاذي الدكتور عصام اسماعيل، واعتبره مرجعية دستورية، الذي شجعني على المضي في بحثي بالرغم من قلة المراجع باللغة العربية، والذي وفر لي كل الدعم، وكان محفزا.

كل الشكر لثقتك.

المقدمة

يرتبط الحق بالخصوصية بالحرية الشخصية ويشكل مدماكا اساسيا للديمقراطية كما يتصل اتصالا وثيقا بالحق في حماية البيانات الشخصية والحق في الوصول الى المعلومات مع احترام عدم التدخل بالحياة الشخصية. تعتبر الخصوصية اذا من اساسيات الكرامة الانسانية اذ يصعب تخيل حياة الافراد اذا ما كانوا مراقبين دوما ويمكن الاعتماد على درجة تمتع الافراد بالخصوصية كمؤشر للديمقراطية والحرية.

هذا الحق كفلته المواثيق الدولية لاسيما المادة ١٢من الاعلان العالمي لحقوق الانسان والمادة ١٧ من العهد الدولي الخاص للحقوق المدنية والسياسية بحيث لا يجوز التدخل التعسفي في خصوصيات الفرد او اسرته او منزله او مراسلاته ولكل شخص الحق في حماية القانون من هذا التدخل. هذا فضلا عن ان الكثير من الدول أدخلت الحق في الخصوصية ضمن دساتيرها والعديد من الاجهزة الحكومية اعتمدت سياسات خصوصية شفافة وواضحة لضمان حماية المعلومات الشخصية التي يتم جمعها، اذ يجب الاعتراف ببعض الحقوق للافراد في ما يتعلق ببياناتهم الشخصية وايجاد آليات رقابة وملاحقة تضمن حماية هذه البيانات وحق اصحابها في الوصول اليها والقيام بالتصحيحات المناسبة عند الاقتضاء.

غير انه لا شك ان مختلف الحقوق الاساسية تقتضي وجود استثناءات يجب حصرها وتفسيرها بالمفهوم الضيق في اطار ضرورة حماية الامن القومي او النظام العام او حقوق الآخرين وحرياتهم. لذا من واجب الدول ضمان احترام هذه المبادئ وملاحقة من لا يحترمها.

يزداد اهمية طرح هذا الموضوع مع التطور التكنولوجي الذي بلغه عصرنا الرقمي اليوم والبيانات الكبيرة التي يتم جمعها ان من الدولة او من الشركات الخاصة، بحيث اصبحت بياناتنا الشخصية اليوم في كافة الادارات العامة من اجهزة امنية ودوائر مالية وصحية واجتماعية مع ما يرافق ذلك من بيانات بيومترية وغيرها. هذا فضلا عن البعد الامني لاسيما ان الحكومات تنحو الى التوسع في عمليات التنصت وجمع البيانات الشخصية بهدف مكافحة الارهاب مع ما يعنيه ذلك من مراقبة لحركة الاتصالات وزيادة كاميرات المراقبة وكشف المعطيات والبيانات الشخصية، كل ذلك مع سهولة اكبر في الادوات التي تتيح التنصت وجمع البيانات بسبب التطور التكنولوجي

والبرمجيات الحديثة. هذا فضلا عن تنامي الابتكار في المجال الرقمي وازدياد التطبيقات والشركات التي تجمع بياناتنا الشخصية وتخلق لنا هويات رقمية وتتتبع تحركاتنا وتؤثر حتى على حقنا بالتعبير وتبيع بياناتنا لاغراض تسويقية وتجارية. تقتضي هذه التحديات الجديدة الناتجة عن طبيعة الانترنت العابر للحدود الوطنية توفير ضمانات على المستوى الوطني المحلي وكذلك التعاون الدولي بين كافة أصحاب المصلحة لايجاد حلول فعالة لحماية خصوصية المواطنين وبياناتهم الشخصية.

لم تكن حماية الخصوصية والبيانات الشخصية تحتل اهمية كبرى لدى المشرع اللبناني قبل صدور قانون المعاملات الالكترونية وحماية البيانات الشخصية رقم ٨١ تاريخ ١٠ تشرين الاول ٢٠١٨ بعد ان تقاذفته اللجان البرلمانية منذ العام ٢٠٠٤. حتى ان الدستور اللبناني لم يتضمن موادا صريحة لحماية الخصوصية والبيانات الشخصية وانما اكتفى بالاشارة في المادة ٨ الى ان الحرية الشخصية مصونة وفي حمى القانون، كما شدد في المادة ١٤ على خصوصية المنزل وحرمته. هاتان المادتان فضلا عن التزام لبنان بالمواثيق الدولية شكلتا اساسا لبعض الاجتهادات في اطار ايجاد ضمانات للخصوصية وحماية البيانات الشخصية. كما يمكن ايجاد بعض القوانين التي تطرقت لهذا الحق مثل القانون رقم ٩٩/١٤٠ الذي يتعلق بحماية جميع انواع التخابر والاتصال وقانون الحق بالوصول الى المعلومات الذي أقر مؤخرا في ٢٠١٧ ويتضمن في مادته الرابعة احكاما تتعلق بالمستندات الادارية المتعلقة بمعلومات ذات طابع شخصي.

انطلاقا من هذه الوقائع، نحاول في هذه الرسالة الاجابة على الاشكالية التالية: **هل هناك اطار قانوني واضح يضمن الحق بالخصوصية وفي حماية البيانات الشخصية في لبنان وفق المعايير الدولية وهل تتيح هذه القوانين آليات واضحة لصون هذا الحق الاساسي وحمايته؟**

فهل اوجدت هذه القوانين آليات واضحة وفعالة يمكن لاي متضرر ان يتخذها في حال وجد ان خصوصيته قد انتهكت؟ وهل وضعت هذه القوانين آليات رقابية على الادارة نفسها في حال تم خرق موجب حماية البيانات الشخصية؟ وقد مرت عدة حوادث مثل تسريب تطبيق باسم مالك السيارة وهاتفه عند ادخال رقم السيارة ما ينتهك خصوصية الافراد وغيرها من الحوادث مثل انتهاك الحكومة اللبنانية لخصوصية اللبنانيين عبر تسليم كافة البيانات

الخاصة بالاتصالات للاجهزة الامنية منذ العام ٢٠١٢. اضافة الى المعلومات الشخصية التي يطلع عليها مزودو خدمات الانترنت دون اي آليات رقابية تضمن حماية هذه البيانات. فضلا عن فضيحة "دارك كاراكال" التي كشفت تجسس الامن العام على اللبنانيين وتم التعاطي معها باستخفاف من قبل المراجع اللبنانية الرسمية. كل تلك الحوادث دون ان يستدعي ذلك فتح نقاش جدي حول آليات صون حق الخصوصية وحماية البيانات الشخصية. يأتي كل ذلك في وقت تنحى كافة الدول الديمقراطية الى مقاربة أكثر فعالية لموضوع حماية الخصوصية والتعامل مع البيانات الكبيرة وحمايتها لاسيما بعد اللائحة العامة لحماية البيانات GDPR الصادرة عن البرلمان الاوروبي والتي دخلت حيز التنفيذ في ايار ٢٠١٨.

لذا اخترنا هذا الموضوع نظرا لمساسه باحدى الحريات الاساسية وقصور اي نقاش جدي او رؤية لاطار قانوني واضح يتيح آليات واضحة لصون هذه الحقوق.

انطلاقا من موجب الدول تأمين حماية الخصوصية والبيانات الشخصية وموجب مراقبة الشركات الخاصة ومزودي الخدمات لناحية تعاملها مع هذه البيانات الشخصية وحمايتها، سنحاول ان نحدد المنظومة القانونية التي ترعى موضوع الخصوصية في لبنان وما هو موقف الاجتهاد اللبناني في ضوء المعايير الدولية. هل هناك ضمانة دستورية لحق الخصوصية في لبنان؟ وما هي القوانين التي تتناول الخصوصية؟ وكيف تتعامل الادارة اللبنانية مع هذا الموضوع وهل يشكل هاجسا تأخذه بعين الاعتبار في ممارساتها في اطار تنفيذ مهامها؟ وهل تتداخل حقوق اخرى مع الحق بالخصوصية، لاسيما حق المواطنين بالاطلاع والحق بحرية التعبير وحرية الاعلام؟ سنحاول الاجابة في الفصل الاول من هذه الدراسة على هذه الاسئلة انطلاقا من تشريح حماية الخصوصية في القانون اللبناني في ضوء القوانين المقارنة التي وضعت اسسا لحماية هذا الحق والمعايير التي يجب مراعاتها ان في طبيعة هذا الحق او ضمانات حمايته او تداخله مع حقوق اساسية اخرى. كما سنستلهم ببعض الاجتهادات عند توافرها للوقوف عند مبادئ متعلقة بالحق بالخصوصية كما رسختها المحاكم الدولية وسنستعرض تعامل الاجتهاد اللبناني مع الموضوع وذلك رغم ندرة الاجتهادات التي تتعلق بحماية الخصوصية كحق اساسي. ويشكل ذلك مؤشرا

الى ضعف الوعي على هذا الحق الاساسي الذي لا يشكل اولوية ليس فقط لدى المشروع وانما ايضا لدى المواطنين اللبنانيين.

كما سنحاول في الفصل الثاني استعراض حماية البيانات الشخصية بين القانون والممارسة والتجارب المقارنة. ويرتدي هذا الفصل لاسيما في مبحثه الثاني اهمية لجهة حداثة القوانين التي ترعى حماية البيانات الشخصية في لبنان ان لجهة قانون الوصول الى المعلومات الذي اقر في ٢٠١٧ او لجهة قانون المعاملات الالكترونية وحماية البيانات الشخصية الذي اقر في العام ٢٠١٨.

فهل تضع هذه القوانين أطرا واضحة لكيفية تعامل الادارات مع هذه البيانات الشخصية؟ ما هو موقف الاجتهاد اللبناني وما مدى استخدام المواطنين لحقهم بالتقاضي لحماية حقهم بالخصوصية وبحماية بياناتهم؟ كل هذا ستتم معالجته عبر اعتماد المنهج المقارن لاسيما بالنظر الى المبادئ التي تم ارساؤها حديثا لاسيما مع ايلاء الامم المتحدة اهمية اكبر للموضوع عبر آلية مستحدثة في ٢٠١٥ لتعزيز الحق في الخصوصية وهي مقرر خاص لدى الامم المتحدة حول الحق في الخصوصية، فضلا عن الاتحاد الاوروبي الذي أولى موضوع الخصوصية والبيانات الشخصية اهتماما كبيرا وقد حدّث مؤخرا الاطر التنظيمية لحماية البيانات الشخصية ودخلت حيز التنفيذ في ايار عام ٢٠١٨ عبر اللائحة العامة لحماية البيانات الشخصية GDPR. هذا فضلا عن استحضار تجارب مثل التجربة الفرنسية التي تولي اهمية قصوى لموضوع الخصوصية وحماية البيانات الشخصية وذلك منذ زمن بعيد وحتى قبل الفورة التكنولوجية، حيث تم انشاء اللجنة الوطنية للمعلوماتية والحريات (CNIL) في العام ١٩٧٩، وهي هيئة ادارية مستقلة ناظمة تعنى بضبط البيانات الشخصية وهي تساهم اليوم في رفد النقاش واقتراح آليات تنظيمية لموضوع التعامل مع البيانات في هذا العصر الرقمي وتقوم بمهام الهيئة المستقلة المشرفة على حماية البيانات ضمن اطار اللائحة العامة لحماية البيانات الشخصية. كما سنعتمد على معايير ارستها منظمات معروفة بدفاعها عن حق الخصوصية مثل "الخصوصية الدولية" Privacy International وغيرها من المنظمات التي تشارك في النقاش العام على المستوى الدولي. كما ان اعتماد المنهج المقارن يضعنا امام حلول جديدة تعتمدها دول تعلي شأن الحق بالخصوصية وحماية البيانات الشخصية وتعتبرها من الحريات الاساسية الواجب صونها كما ان لديها

قدرات اوسع لمواكبة التطور التكنولوجي والتحديات التي يطرحها إزاء موضوع الخصوصية والبيانات الشخصية. فيكون بالتالي من المفيد النظر الى القانون المقارن لاستيقاء ما يتلاءم مع سياقنا العام ومجتمعنا وروحية دستورنا وقوانيننا صونا للحريات الاساسية التي تضمن كرامة الانسان.

التصميم العام:

مقدمة

الفصل الاول: الخصوصية في القانون اللبناني والمقارن

المبحث الاول: الاطار النظري لمفهوم الخصوصية

المبحث الثاني: الضمانة الدستورية والقانونية للخصوصية في لبنان وفي القانون المقارن

المبحث الثالث: الخصوصية وحق المواطنين بالاطلاع

الفصل الثاني: حماية البيانات الشخصية بين القانون والممارسة والتجارب المقارنة

المبحث الاول: آليات حماية البيانات الشخصية في القانون المقارن

المبحث الثاني: القوانين اللبنانية الحالية التي تحمي البيانات الشخصية

المبحث الثالث: التعامل مع البيانات الشخصية في الواقع اللبناني

الخاتمة

الفصل الاول: حماية الخصوصية في القانون اللبناني والمقارن

تعد الخصوصية حقا من الحقوق الاساسية وان كان من الصعب تعريف مضمون هذا الحق بشكل دقيق كسائر الحقوق الاساسية الاخرى. وبالرغم من تشكل هذا الحق منذ فترة بعيدة الا ان التطور التكنولوجي وسرعة التغيرات الرقمية على كافة المستويات العامة والخاصة جعلت الاحاطة بمفهوم الخصوصية وجوانب الحماية اكثر تعقيدا. في حين كان يقتصر التمسك بالخصوصية على صفحات الصحف والمجلات في القرن الماضي اصبحنا اليوم مع الانترنت والتقنيات الحديثة امام واقع مختلف يستدعي فهم ماهية الخصوصية في عصرنا المعاصر وسبل حمايتها. ان التحديات الجديدة التي يخلقها الانترنت فيما يتعلق بحماية الحق في الخصوصية [1] يكمن في التطور التكنولوجي وازدياد الابتكار الذي ادى الى خلق ادوات لجمع العديد من المعلومات الخاصة بالافراد لم يكن بالامكان الحصول عليها سابقا. كما ان البيانات الشخصية للافراد ازدادت باضطراد مع استخدام الحواسيب والهواتف الذكية والتحول الى العمليات الرقمية فاصبح هناك لكل فرد هوية رقمية تتضمن عنوان بروتوكول انترنت فريد IP وبيانات شخصية مخزنة في اجهزة وسحابات cloud عديدة. هذا الواقع اعطى ايضا قدرات اضافية للحكومة والقطاع الخاص لتحليل البيانات الشخصية المخزنة لديها كما شكل فرصة للاستخدام التجاري والتسويقي للبيانات الشخصية. ويشكل هذا الامر التحدي الاكبر لاسيما انه يعتبر نموذج عمل معظم الشركات وضمنها التي تدير مواقع التواصل الاجتماعي التي تقدم خدماتها مجانا لقاء الاستفادة من البيانات المجمعة لديها لاغراض تجارية.

سنعالج في هذا الفصل الاطار النظري لمفهوم الخصوصية في المبحث الاول عبر محاولة تعريف هذا المفهوم استنادا الى المواثيق والمعاهدات والآليات الدولية وآراء الفقهاء والقانونيين، وعبر تشريح طبيعة هذا الحق الذي يتعلق بالحريات الاساسية. وسننتقل في المبحث الثاني الى تفصيل الضمانة الدستورية والقانونية للخصوصية في لبنان وفي القانون المقارن. هذه الضمانة متمثلة في مجموعة قوانين حاولنا تفنيدها حسب المواضيع التي تعالجها مستندين الى ما تضعه المعايير الدولية من اطر لحماية هذا الحق. كما خصصنا المبحث الثالث لتداخل

---

[1] توبي مندل وآخرون، دراسة استقصائية عالمية حول خصوصية الانترنت وحرية التعبير، منشورات اليونسكو، ص ٧

الحق بالخصوصية مع حقوق اساسية اخرى تتعلق بحق المواطنين بالاطلاع وذلك عبر رسم الحدود بين حرية التعبير والخصوصية واستعراض موقف الاجتهاد اللبناني والمقارن على قاعدة مبدا سمو المصلحة العامة.

المبحث الاول: الاطار النظري لمفهوم الخصوصية

نستعرض في المطلب الاول من هذا المبحث تعريف مفهوم الخصوصية على ضوء متغيرات مستجدة لاسيما تعيين مقرر خاص لدى الامم المتحدة حول الحق في الخصوصية في ٢٠١٥ وعلى ضوء اجتماع خبراء في مكتب المفوضية العليا لحقوق الانسان في جنيف في شباط ٢٠١٨، حول الحق في الخصوصية في العصر الرقمي. ونعود الى تاريخ نشوء الحق في الحياة الخاصة بمفهومه التقليدي في النصف الثاني من القرن التاسع عشر وكيف تبلورت في القرن العشرين. كما نورد تعريفات كل من الاعلان العالمي لحقوق الانسان والعهد الدولي الخاص للحقوق المدنية والسياسية. وفي المطلب الثاني نستعرض تعلق هذا الحق بالحريات الاساسية عبر الاضاءة على أبرز اوجه الخصوصية من خصوصية المعلومات الى الخصوصية الجسدية الى خصوصية المراسلات والخصوصية الاقليمية لمحاولة فهم كل جوانب هذا الحق.

المطلب الاول: تعريف مفهوم الخصوصية

بدأ مؤخرا الحق بالخصوصية يحتل اهمية اكبر في العالم في ظل التطور الرقمي، لاسيما في الامم المتحدة. فقد أدت قرارات حول الحق بالخصوصية في الهيئة العامة للامم المتحدة عامي ٢٠١٣ و ٢٠١٤ الى تأسيس مجلس حقوق الانسان آلية خاصة لتعزيز وحماية الخصوصية، وهي مقرر خاص لدى الامم المتحدة حول الحق في الخصوصية[2] وذلك في آذار عام ٢٠١٥، قرار رقم ٢٨/١٦. كما بدأ مقررون خاصون آخرون فضلا عن مجلس حقوق الانسان يسائلون الدول اكثر فاكثر لاسيما في المراجعات الدورية حول حماية الخصوصية ويوردون في توصياتهم مخاوف حول ازدياد التنصت ما يخرق حقوق الانسان.

---

[2] موقع المفوضية العليا لحقوق الانسان في الامم المتحدة،
https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

وتدخل ضمن مهام المقرر الخاص حول الحق في الخصوصية الأمور التالية:

- جمع المعلومات والقيام بالتوصيات لضمان وتعزيز الحق في الخصوصية، وضمنها ما يتعلق بالتحديات الناتجة عن التكنولوجيا الحديثة.

- تقديم تقارير حول اعتداءات مشكو منها على حق الخصوصية، اينما حصلت، وذلك كما تحددها المادة ١٢ من الاعلان العالمي لحقوق الانسان والمادة ١٧ من العهد الدولي الخاص للحقوق المدنية والسياسية.

- تحديد وتبادل وتعزيز المبادئ والممارسات الفضلى على المستويات المحلية والاقليمية والدولية وتقديم الاقتراحات والتوصيات الى مجلس حقوق الانسان.

- رفع الوعي حول اهمية تعزيز وحماية الحق بالخصوصية.

وتشمل نشاطات المقرر الخاص التواصل مع الحكومات مثل ارسال شكوى اورسائل عاجلة حول انتهاكات مشكو منها تتعلق بالحق بالخصوصية او اصدار بيانات صحافية لابداء القلق حول امور معينة مثل التعليق على قانون جديد لدولة معينة او اي تطور آخر يؤثر على الحق بالخصوصية. كذلك يمكن للمقرر ان يقوم بزيارات للبلدان المعنية للوقوف عند وقائع معينة. كما يصدر تقارير سنوية الى مجلس حقوق الانسان والهيئة العامة، تتضمن تحليلا وتوصيات حول مواضيع محددة مرتبطة بالحق بالخصوصية.

ان النقاش في الحق في الخصوصية في السنوات الاخيرة ازدادت اهميته خاصة مع تنامي سياسات او ممارسات المراقبة والتنصت التي تقوم بها الحكومات حول العالم. وكانت الهيئة العامة للامم المتحدة في قرار ٦٨/١٦٧ عام ٢٠١٣ قد أبدت تخوفها الشديد من الأثر السلبي للتنصت على حقوق الانسان.[3] كما شددت الهيئة العامة على ان الحقوق التي يتمتع بها الافراد في الحياة العادية يجب ان تتمتع بنفس الحماية على الانترنت ودعا الدول الى تأمين حماية الخصوصية في زمن التواصل الرقمي. ان الاعتداءات الارهابية

---

[3] البند ١٠٢ من رسالة المقرر الخاص حول الحق في الخصوصية الى المفوضية العليا لحقوق الانسان، https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UN_SRP_Letter_to_OHCHR_8June.pdf

في العديد من الدول ومنها الديمقراطية مثل فرنسا والمانيا وبلجيكا وبريطانيا أعطت الاولوية في الكثير من الحالات الى تدابير امنية وفق مقاربة لا تؤمن التوازن بين الامن وحماية خصوصية المواطنين. وتنحى الحكومات الى التهرب من مناقشة مدى تطابق تشريعاتها الوطنية المتعلقة بالمراقبة والتنصت مع المعايير الدولية لحماية الحق في الخصوصية، وذلك رغم كون هذا النقاش في صلب الحياة العامة لاسيما بعد سلسلة اعترافات من موظفين سابقين في وكالات الامن القومي مثل "ادوارد سنودن" حول ممارسات الدول فيما يتعلق بالتنصت وانتهاكها للحق بالخصوصية.

في ورقة تم تقديمها في اجتماع خبراء في مكتب المفوضية العليا لحقوق الانسان في جنيف في شباط ٢٠١٨، حول الحق في الخصوصية في العصر الرقمي، تم تعريف الخصوصية انها حق اساسي من حقوق الانسان معترف فيه في القانون الدولي. كما انه حق عالمي، يتمتع به الجميع في كل مكان، ويجب احترامه من الجميع وفي كل مكان، من قبل الدول وكذلك الفاعلين من غير الدول، بغض النظر عن الجنسية او الاثنية او الدين او الجندر او المعتقدات الفلسفية والسياسية. كما ان الاعتراف بهذا الحق الدولي هو جزء من النظم الاساسية في تطور قوانين حقوق الانسان منذ الحرب العالمية الثانية.

نظرا لتداخل الحق في الخصوصية في سياقات عديدة مثل الصحة، الاحصائيات، الامن القومي، المالية، الشرطة، الضمانات الاجتماعية وغيرها يتطلب الحق في الخصوصية اطرا قانونية تفصيلية في كل من هذه السياقات. لكن المفارقة انه لا يوجد تعريف موحد عالميا للخصوصية. هناك اجماع حول العالم على تكريس الحق في الخصوصية وان الجميع يتمتع بهذا الحق، غير انهم لم يحددوا بالتفصيل ما هو هذا الحق او ماذا يخول الشخص ان يتمتع به في كل حالة. ان هذا الواقع يجعل من التعريف الضيق للخصوصية يحد من هذا الحق في ظل المتغيرات التي نشهدها كما ان الاحاطة بكافة هذه الظروف المتغيرة فيها من الصعوبة مثل استخدام الهواتف الذكية وبطاقات الائتمان والانترنت بشكل عام. لذا اضاءت ورقة جنيف المذكورة على اطر قانونية ضمن القانون الدولي يمكن للقوانين المحلية الاستناد عليها.

اكثر من ٣٣ ٪ من الدول الاعضاء في الامم المتحدة (اكثر من ٧٠ دولة) ليس لديهم قوانين تتعلق بالخصوصية [4]، اما باقي الدول ال١٢٥ لديهم شكل من اشكال القوانين ولكن بنسب متفاوتة لجهة مواصفات اساسية مثل وجود هيئات حماية مستقلة. كما ان اكثر من ٨٠٪ من الدول الاعضاء في الامم المتحدة لا يوجد فيها قوانين تحمي الخصوصية عبر تنظيم متناسب ورقابة واضحة لاستخدام ادوات التنصت محليا.

وحدها البلدان الاوروبية التي رعاها المجلس الاوروبي وافقت على انه يمكن لتدابير معينة ان تحد من الحق في الخصوصية فقط اذا كانت هذه التدابير منصوص عنها في القانون وهي تعتبر ضرورية ومتناسبة في مجتمع ديمقراطي. وتعيد اليوم هذه الدول النظر بتشريعاتها لتوفير حماية اكبر للحق في الخصوصية. لقد ادت التقنيات الحديثة الى تبلور مفهوم الخصوصية وتوسعه بعد ان كان محصورا في اماكن اكثر وضوحا مثل حماية المسكن والحياة الاسرية. ثم جاءت تكنولوجيا الاتصالات لتجلب معها مزيدا من التحديات المرتبطة بمراقبة الاشخاص.

لم يظهر الحق في الحياة الخاصة بمفهومه التقليدي الا في النصف الثاني من القرن التاسع عشر. في عام ١٨٥٥ منع رئيس المحكمة المدنية لمدينة السين في فرنسا بقرار قضائي معجل عرضا علنيا للوحة تظهر فيها مدبرة اخوات الرعاية. وبعد ثلاث سنوات في العام ١٨٥٨ في قضية راشيل عاقبت المحكمة المدنية للسين نشر صورة للفنان على فراش الموت [5].

ان المخاوف المتعلقة بالتعدي على الخصوصية ليست جديدة اذا ويمكن القول انها تبلورت بوضوح في القرن العشرين لاسيما في الورقة التي اعدها "Samuel Warren" و"Louis Brandeis" بعنوان "الحق

---

[4] تقرير المقرر الخاص حول الحق بالخصوصية A/HRC/37/62، مقدم الى مجلس حقوق الانسان في جلسته السابعة والثلاثين المنعقدة بين ٢٦ شباط و٢٣ آذار ٢٠١٨، shorturl.at/zXY57

[5] الاستاذ اندريه برتران والمحامي الدكتور نقولا فتوش، الحق في الحياة الخاصة والحق في الصورة، دار صادر، ٢٠٠٣، ص ٣٠

في الخصوصية" في العام ١٩٨٠،والتي أعدت في وقت كانت الصحف تنشر فيه صور الاشخاص للمرة الاولى. وقد عرفا الخصوصية بانها " الحق في أن يخلى المرء وشأنه" .[6]

عرف "Alan Westin"، مؤلف "الخصوصية والحرية" في ١٩٦٧، الخصوصية على انها رغبة الناس في ان يقرروا بحرية وفق اية ظروف والى اي مدى يريدون عرض انفسهم وسلوكهم وتصرفاتهم للآخرين. [7]

وفق Ruth Gavison هناك ٣ عناصر للخصوصية: السرية، الهوية المغفلة anonymity والوحدة. هي حالة يمكن ان تتم خسارتها بخيار الشخص نفسه او بفعل من شخص آخر .[8]

وفي فرنسا شكل قانون ١٧ تموز ١٩٧٠ منعطفا لتعزيز ضمان حقوق المواطنين الشخصية وفيه ان "لكل انسان الحق في احترام الآخرين لحياته الخاصة ."[9]

ويشمل هذا الحق عدة سياقات منها حماية حرمة المنزل فلا يمكن مثلا للشرطة الدخول الى المنزل الا في حالات محددة في القانون، السرية المهنية والطبية فلا يمكن لطبيب مثلا ان يكشف حالة المريض الصحية دون موافقته، وحماية الحياة الخاصة مثل العلاقات العاطفية وحماية الحق في الصورة فلا يمكن تداول الصورة دون موافقة الشخص المعني طبعا في حدود مراعاة الصور في الاجتماعات العامة او المتعلقة بالحياة العامة للاشخاص العامين. هذا فضلا عن التنصت على الاتصالات التي لا يمكن اجراؤها الا بقرارات قضائية في حالة التحقيق في الجرائم مثلا كذلك ضرورة تنظيم حالات التنصت من الاجهزة الامنية لغايات مكافحة الارهاب.

---

[6] Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin and Nathalia Torres, Global Survey on Internet Privacy and Freedom of Expression, UNESCO Series on Internet Freedom, p. 9

[7] Alan Westin, Privacy and Freedom 7 (1967)

[8] Ruth Gavison, Privacy and the Limits of Law, 89 Yale 421 (1980)

[9] نص القانون على موقع Legifrance، رابط
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000693897

ان تعريف الخصوصية على المستوى الدولي وجد عام ١٩٤٨ في الاعلان العالمي لحقوق الانسان والذي حمى تحديدا الخصوصية الاقليمية وخصوصية المراسلات. وقد نصت المادة ١٢ على ما يلي:

"لا يجوز تعريضُ أحد لتدخُّل تعسُّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حقٌّ في أن يحميه القانون من مثل ذلك التدخُّل أو تلك الحملات."

كما تشير العديد من المعاهدات الدولية الى الخصوصية كحق من حقوق الانسان ومنها العهد الدولي الخاص للحقوق المدنية والسياسية ومعاهدة الامم المتحدة حول العمال اللاجئين ومعاهدة الامم المتحدة حول حقوق الطفل.

وقد نصت المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية على التالي:

1. لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.
2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس.

اما على على المستوى الاقليمي فهناك معاهدات عديدة يمكنها ان تشكل اطارا قانونيا ملزما مثل معاهدة حماية حقوق الانسان والحريات الاساسية [10] في مادتها الثامنة:

" (1)لكل فرد الحق في احترام حياته الخاصة والعائلية ومنزله ومراسلاته. (2) لن يكون هناك تدخل من جانب سلطة عامة في ممارسة هذا الحق إلا وفق القانون على ان يكون ضروريا في مجتمع ديمقراطي لصالح الأمن القومي أو السلامة العامة أو الرفاهية الاقتصادية للبلد، للوقاية من الاضطراب أو الجريمة، لحماية صحة الأخلاق، أو لحماية حقوق وحريات الآخرين."

---

[10] **CONVENTION FOR THE** PROTECTION **OF** HUMAN RIGHTS **AND FuNDAMENTAL** FREEDOMS Rome, http'J/www.coe.fr/eng/legaltxt/5e.htm

وفي مراجعة هذه المادة من الهيئة الاوروبية لحقوق الانسان ومن المحكمة الاوروبية لحقوق الانسان رأت الهيئة ان الحق في احترام الحياة الخاصة لا ينتهي هنا. بل يشمل الى حد ما، حق بناء وتطوير علاقات مع افراد آخرين لاسيما في الحقل العاطفي لتطوير شخصية كل فرد .[11]

كما فرضت المحكمة الاوروبية على العديد من الدول الاعضاء عقوبات لفشلها بتنظيم المراقبة والتنصت من قبل الحكومات وغير الحكومات.

المطلب الثاني: طبيعة الحق بالخصوصية وتعلقه بالحريات الاساسية

لا شك ان الخصوصية هي الاصعب تعريفا بين حقوق الانسان على المستوى الدولي. للخصوصية جذور عميقة في التاريخ. لقد ذكرت في الكتاب المقدس مرات عديدة كما في الديانة اليهودية والموروث الاغريقي والصيني القديم. وكانت حماية الخصوصية ترتبط بالحق بالوحدة. تختلف تعريفات الخصوصية بين البلدان حسب السياق والبيئة، وقد تم دمجها احيانا مع البيانات الشخصية اذ ترتبط بادارة البيانات الشخصية. خارج هذا السياق فان الخصوصية هي "طريقة لرسم الخط حول مدى امكانية المجتمع من التدخل في شؤون شخص ما [12]."

ويرتبط الحق بالخصوصية بالعديد من القضايا المهمة، مثل الحرية والحق في مساحة شخصية منفصلة عن الفضاء العام، والحق في الوصول من دون الكشف عن المعلومات الشخصية. كما انه مرتبط بمفاهيم الهوية والسرية والكرامة الانسانية. فضلا عن الحق في حماية البيانات الشخصية والملكية الفكرية والامن الرقمي. [13]

يمكن تقسيم الخصوصية حسب المنظمة الدولية لحماية الخصوصية الى الاوجه التالية:

---

[11] X v. Iceland, 5 Eur. Comm'n H.R. Dec. & Rep. 86, 87 (1976).

[12] Simon Davies, Big Brother: Britain's Web of Surveillance and the New Technological Order 23 (1996)

[13] حرية الانترنت في لبنان، مؤسسة مهارات ومكتب اليونسكو بيروت، ٢٠١٥، ص ٣٩

- خصوصية المعلومات: وتتضمن وضع قواعد تجميع وحفظ ومعالجة البيانات الشخصية مثل البيانات الطبية او المعلومات الائتمانية.
- الخصوصية الجسدية: تتعلق بحماية الاشخاص الجسدية بوجه الاجراءات التدخلية invasive مثل فحص المخدرات او تفتيش الاعضاء الجسدية.
- خصوصية المراسلات وهي تشمل خصوصية وامن الاتصالات والايميلات والرسائل واي شكل من اشكال التواصل.
- الخصوصية الاقليمية وتتعلق بوضع حدود للتسلل الى المنزل او اي بيئة اخرى مثل مكان العمل او المكان العام.

عدم وجود تعريف واحد للخصوصية لا يلغي من اهمية هذا الحق لاسيما لارتباط جميع حقوق الانسان فيه. بذلك تكون الخصوصية حقا من الحقوق الاساسية الضرورية لحماية الكرامة الانسانية وأساسا تبنى عليه العديد من حقوق الانسان الاخرى. تساعد الخصوصية الافراد في وضع حدود لمن له الحق في الوصول الى جسدهم، الاماكن والاشياء الخاصة بهم فضلا عن مكالماتهم ومعلوماتهم. يتوجب على اي منظومة حماية لهذا الحق ان تؤكد هذا الحق في ظل عدم توازن القوى، اذ ان الخصوصية حق اساسي لحماية الافراد والمجتمع من الاستخدام المفرط والعشوائي لما ينتهك خصوصياتهم، وذلك عبر تقليص ما يمكن معرفته عن الافراد او فعله بهم وفي نفس الوقت توفير الحماية من الآخرين الذين يسعون لممارسة هذه السيطرة.

تتعلق الخصوصية بالحرية الشخصية للافراد اذ تعطيهم المساحة ليكونوا انفسهم دون الخوف من آراء الآخرين واحكامهم كما تخولهم التفكير بحرية دون التعرض للتمييز وهي عنصر مهم يجعل الافراد يتحكمون بما يعرفه الآخرون عنهم.

الخصوصية اذا هي شرط اساسي لممارسة حقوق اساسية مثل حرية التعبير والاستقلالية الشخصية للافراد. هناك ترابط وثيق بين الخصوصية والحرية والكرامة الانسانية. وان احترام خصوصية الفرد يعطيه الحق بان يعبر عن نفسه وبان يعيش بحرية ويعطيه اعترافا بفرديته واستقلاليته كانسان. [14]

وتعتبر المنظمة الدولية للخصوصية ان النقاش حول الخصوصية في المجتمع الحديث مرتبط بالحريات الحديثة. [15]اذ في وقت يفكر الافراد في كيفية وضع وحماية الحدود حولهم وقدرتهم على تقرير ما يحدث لهم فانهم يحاولون ان يضعوا اسسا مرتبطة بثلاثة مستويات:

- اخلاقيات الحياة الحديثة
- الاسس التي تحكم الممارسات التجارية
- والتحفظات التي يجب وضعها مقابل قوة السلطات العامة.

لا شك ان التطور التكنولوجي اليوم جعل التحدي لحماية الخصوصية اكبر لاسيما مع القدرات المتنامية لقدرات التنصت والمراقبة. لقد اصبحنا في عصر يتعاطى مع الافراد كمجموعة بيانات وتصدر القرارات احيانا بناء على كم البيانات حول الافراد. يمكن للحكومات والشركات اليوم ان تراقب كل محادثة يجريها اي فرد، كل معاملة تجارية وكل مكان تتم زيارته. هذه القدرات المتنامية قد تؤدي الى آثار سلبية على الافراد والمجموعات والمجتمعات وتؤثر على العلاقات بين الافراد والاسواق والمجتمع والدولة.

يضع هذا الواقع الافراد في وضع يجعل المؤسسات التي يعتمدون عليها، عامة كانت او خاصة، قادرة على معرفة تاريخهم ومراقبة افعالهم وتكهن افعالهم المستقبلة، ما يؤدي الى عدم توازن القوى التي تؤدي بدورها الى زوال الاستقلالية الفردية الشخصية في وجه الشركات والمجموعات والحكومات حتى سحقها.

---

[14] http://web.simmons.edu/~chen/nit/NIT%2796/96-025-Britz.html

[15] https://privacyinternational.org/explainer/56/what-privacy

تستفيد الدول اليوم من تقنيات المراقبة الحديثة مثل كاميرات المراقبة وبرمجيات التنصت وغيرها لاسيما مع تنامي "الحرب على الارهاب"، وغالبا ما لا تعير هذه الدول اهتماما لقوانين الخصوصية القائمة او مبادئها العامة. وتكمن الخطورة هنا عندما تستخدم الدول هذه التقنيات في مراقبة اعمال المواطنين لاسيما المعارضين لسياساتها.

وما يجعل الخطر اكبر على الخصوصية كحرية شخصية هو عدم تنبه الافراد في غالب الاحيان ما يجعل الدول والشركات تتمادى اكثر في انتهاك هذا الحق وعدم وضع اطر حمائية له.

ان هذا التمادي يتمثل في عدم اهتمام معظم الدول والشركات في اعلام الافراد حول المراقبة التي يمارسونها وعدم قدرة الافراد او تنبههم لمساءلة حكوماتهم حول اطر هذه المراقبة التي غالبا ما تكون سرية تنتهك خصوصية مجموعة كبيرة من الافراد. هذه المراقبة التي تخرق الخصوصيات في ظل نقص في المساءلة تشكل دون شك خطرا داهما على الحياة الديمقراطية وباتت تشكل القاعدة.

لا شك ان الحق بالخصوصية وحماية هذا الحق واجه تحديات كبيرة مع التطورات التقنية الجديدة لاسيما في السنوات الاخيرة وخاصة في تقنيات المعلومات والاتصالات. وما يزيد الامر تعقيدا هو سرعة هذا التطور التكنولوجي الذي غالبا ما يكون اسرع من القوانين وغالبا ما يكون عابرا للحدود وتتداخل فيه اطراف عديدة من شركات ودول.

هذا فضلا عن الدور الكبير الذي يلعبه مزودو خدمات الانترنت والشركات الوسيطة وهم لديهم كافة حركة المستخدمين وكافة بياناتهم وما يترتب على ذلك امكانية تعسفهم في حقهم وانتهاكهم لخصوصية المستخدمين او تعرضهم لضغوطات من حكومات للتعدي على خصوصية المستخدمين ومراقبة تحركاتهم. عادة يخضع مزودو خدمات الانترنت في الدول التي يوفرون فيها هذه الخدمات لتراخيص تضع لهم اطرا لعملهم.

التعقيدات التي فرضها الانترنت تشمل الاستخدام اليومي لمحركات البحث ومواقع التواصل الاجتماعي والهواتف الذكية والتطبيقات وغيرها من الاجهزة. كل ذلك يعقد مسألة تأطير الحق بالخصوصية ويعرضه

للاستغلال لاسيما في الدول القمعية حول العالم التي تستخدم التكنولوجيا والاتصالات لتعقب ومراقبة الافراد.

ثمة كم هائل من الوسائل التقنية لتحديد هوية مستخدمي الانترنت بدءا من التسجيل الاولي من خلال مزودي الخدمات الى ترقيم الاجهزة وتحديد الحسابات المرتبطة بها الى معرفة الهويات الفردية لمتصفحي صفحات الانترنت وعناوين بروتوكول الانترنت وغيرها من اجراءات تسهل اظهار هوية المستخدم. بالرغم من انه في بعض الحالات هناك ضرورة للهوية لتوفير الخدمة ولكن تتجلى المخاوف في البلدان القمعية التي تحد من حرية التعبير حيث يشكل تحديد الهوية قيدا على الخصوصية وسرية الهوية على الانترنت.

هناك تهديدات اخرى امام خصوصية المستخدمين على الانترنت وهي ترتبط ببرمجيات الدعاية التي تعتدي على خصوصية المستخدم وتتجاهل موافقته او "المالوار" والفيروسات وبرامج التجسس التي تستخدم لمراقبة مستخدمين آخرين وتشكل تعديا على الحياة الشخصية للافراد.

اضافة الى برامج مراقبة الحزم وهي قادرة على اختراق الحزم التي تنتقل عبر شبكة الانترنت وهي تعتبر من التقنيات الشائعة في انظمة المراقبة الحكومية. [16]فضلا عن برامج تحديد المواقع الجغرافية لعناوين بروتوكول الانترنت الخاص بالمستخدمين وتسمح لمزودي خدمة الانترنت بتقدير دقيق للموقع الجغرافي الذي يتواجد فيه المستخدم. ويتم تضمين تقنية GPS في العديد من الاجهزة مما يسمح بتحديد دقيق لمواقعها.

المبحث الثاني: الضمانة الدستورية والقانونية للخصوصية في لبنان والقانون المقارن

بعد ان حددنا مفهوم الخصوصية واتصال هذا الحق بالحريات الاساسية سنفصل في هذا المبحث الضمانات الدستورية والقانونية المتوافرة في لبنان في المطلب الاول انطلاقا من اوجه الخصوصية التي عددناها والتي تشمل حرمة المنزل والمراسلات والاتصالات ونستعرض ايضا ممارسة الادارات اللبنانية ومدى احترامها لخصوصية الافراد وذلك عبر استعراض حالتين تتعلقان بتفتيش الهواتف اثناء التحقيق ومدى

---

[16] اللجنة الاوروبية. ٢٠١٠. جدول الاعمال الرقمي. اللجنة تحيل المملكة المتحدة الى المحكمة بشأن حماية الخصوصية والبيانات الشخصية

مراعاة الخصوصية في تطبيقات التتبع الالكتروني لمكافحة وباء كورونا. كما نحاول الاضاءة على ثغرات في الحماية لدى مزودي خدمات الانترنت وغياب اي حماية للحق بالسرية وهو وجه اساسي من اوجه الخصوصية. ونورد في المطلب الثاني المعايير الدولية لحماية الحق بالخصوصية، مشددين على موضوع حماية الاتصالات نظرا للطبيعة الشائكة للتنصت في العالم اليوم، لاسيما التقرير التشاركي "ضروري ومتناسب" الذي يضع ١٣ مبدأ دوليا على تطبيق حقوق الانسان على مراقبة الاتصالات.

المطلب الاول: حماية الحق بالخصوصية في القانون اللبناني

صحيح ان موضوع الخصوصية لم يلق اهتماما كبيرا من المشرع اللبناني الا انه لحظ في نصوص عديدة موضوع حماية الحق بالحياة الخاصة في قوانين متفرقة ان في المسؤولية المدنية او في قانون العقوبات في القدح والذم او غيرها من القوانين. كما ان الدستور اللبناني الذي يصفه نقولا فتوش في كتابه "الحق في الصورة" انه يعكس فكرة "لبنان والحرية توأمان او ان لبنان موئل الحريات وموطنها، او ان الحرية هي سبب وجوده وازدهاره وتفوقه الثقافي". فقد عالج الدستور اللبناني موضوع حقوق الانسان وحرياته الاساسية سواء في دستوره القديم قبل الطائف او بعده. كما ان دستور بعد الطائف اضاف مقدمة تضمنت نصوصا تتعلق بالحقوق الاساسية والاهم التزاما بالمواثيق الدولية ما يعطي هذه المواثيق قيمة دستورية تتفوق على القوانين. تنص المادة الثامنة من الدستور اللبناني على ان "الحرية الشخصية مصونة وفي حمى القانون ولا يمكن ان يقبض على احد او يحبس او يوقف الا وفقا لاحكام القانون. ولا يمكن تحديد جرم او تعيين عقوبة الا بمقتضى القانون." المقصود بالحرية الشخصية حرية الفرد في التنقل كيفما يشاء داخل الدولة وخارجها. وحق الامن بحمايته من كل توقيف او معاقبة الا في الاحوال المعينة التي ينص عليها القانون. بمعنى اوسع الحق بالحياة الخاصة. [17]ويكون الدستور اللبناني قد كرس مبدأ شرعية الجرائم والعقوبات واوجب التقيد بالاحكام العامة المتعلقة بالحرية الشخصية والا عد عملهم تعديا على الحريات.

[17]الحق في الصورة، مرجع مشار له سابقا، ص ٣٤٥

كما يدخل في عداد الحرية الشخصية المصونة في الدستور سرية المراسلات البريدية والمحادثات الهاتفية وغيرها من وسائل التواصل والاتصال، ما يعني انه لا يمكن مصادرتها او مراقبتها الا بامر قضائي.

ونفصل في هذا المطلب الحماية للاوجه المتعددة التي ذكرناها لحق الخصوصية بدءا بحماية حرمة المنزل وحماية المراسلات والاتصالات منعا للتنصت ونستعرض حالات تعاطي الادارة والسلطات الامنية ان في التفتيش اثناء التحقيق او في تطوير الادوات التكنولوجية مثل تطبيقات التتبع الالكتروني، حيث نوثق الانتهاكات في هذا الاطار. ونستعرض ايضا واقع مزودي خدمات الانترنت الذين يستحوذون على الكثير من المعلومات الخاصة بالمستخدمين وغياب الاطر الناظمة لعملهم. واخيرا نذكر حقا اساسيا مرتبطا بالخصوصية وهو الحق بالسرية والغياب التشريعي حوله.

أولا: حماية حرمة المنزل

نصت المادة ١٤ من الدستور على ان "للمنزل حرمة ولا يسوغ لاحد الدخول اليه الا في الاحوال والطرق المبينة في القانون." ما يعني ان تفتيش المنزل من قبل السلطات المختصة يجب ان يستند الى سبب مشروع ووفق الاطر القانونية والقضائية المرعية.

اذا ان تفتيش المنزل بغير ارادة الشخص المعني رغما عنه يمس حرمة يحميها الدستور. بالتالي فان اي تفتيش للمنزل يجب ان يراعي الاحكام القانونية بهدف الحصول على ادلة حول جريمة معينة.

تضمن القانون اللبناني أحكاماً ترعى تفتيش المنزل خلال التحقيق الأولي والتحقيق القضائي ويضع أحكاما خاصة ترعى التفتيش الذي يتناول المحامي.

خلال التحقيق الاولي، تجيز المادة 33 من أصول المحاكمات الجزائية للنائب العام أن يدخل إلى منزل المشتبه فيه للتفتيش عن المواد التي يقدر أنها تساعد على إنارة التحقيق، أن يضبط ما يجده منها وينظم محضراً بما ضبطه واصفاً إياها، بدقة وتفصيل وان يقرر حفظ المواد المضبوطة بحسب طبيعتها.

للنائب العام أن يكلف ضابطًا عدليًا بإجراء التفتيش في منزل المشتبه فيه أو المدعى عليه تحت إشرافه ومراقبته ووفقا للأصول التي يتبعها النائب العام نفسه.

كذلك تجيز المادة نفسها للضابط العدلي إذا وقعت جريمة مشهودة سندًا لأحكام المادة 41من قانون أصول المحاكمات الجزائية، أن يجري التفتيش في منزله ويضبط ما يعثر عليه من مواد جرمية أو أشياء ممنوعة. إذارأى الضابط العدلي أن ثمة أوراقا أو أشياء تفيد التحقيق موجودة لدى شخص لم تتوافر شبهات قوية ضده فيكون للنائب العام أو لقاضي التحقيق، دون الضابط العدلي، أن يجري التفتيش في منزل هذا الشخص ما لم يوافق هذا الأخير دون إكراه على أن يقوم الضابط العدلي بالتفتيش.

كما يجيز القانون دخول المنزل لتنفيذ مذكرات الإحضار وقرارات التوقيف لمن كلف، من قوى الأمن، بتنفيذ مذكرة الإحضار أو قرار التوقيف الغيابي. هنا يمكن لعنصر القوى الامنية المكلف أن يدخل المنزل الذي يمكن ان يكون المدعى عليه قد لجأ إليه وفق الادلة المتوافرة. إنما لا يجوز دخوله إلا في الفترة الممتدة بين الخامسة صباحًا والثامنة ليلا الا اذا وافق صاحب المنزل صراحة على جواز التفتيش خارج هذه الفترة.

في إجراءات التفتيش، يجري التفتيش بحضور المشتبه فيه أو المدعى عليه او بحضور وكيله أو اثنين من أفراد عائلته الراشدين أو شاهدين يختارهما النائب العام.

وقد وضع القانون قواعد لملاحقة من يخالف اصول التفتيش في المنزل وجعله كل تفتيش خلافا للاصول باطلا. يتعرض الضابط العدلي الذي يدخل المنزل، خلافا لأصول التفتيش، للملاحقة بالجنحة المنصوص عليها في المادة 370 من قانون العقوبات غير أن الإبطال في هذا الشأن يقتصر على المعاملة الباطلةولا يتعداه إلى سائر إجراءات التحقيق.

وقد حدد قانون أصول المحاكمات الجزائية اجراءات التفتيش وضبط الأدلة خلال التحقيق القضائي حيث اجاز لقاضي التحقيق أن ينتقل مع كاتبه لتفتيش احد المنازل بحثا عن مواد جرمية أو أشياء تنير التحقيق وعليه أن يعلم النائب العام بانتقاله. كما حدد القانون اصول ضبط المواد والاشياء بحسب طبيعتها وان

كانت وثائق سرية لا يطلع عليها سوى قاضي التحقيق وصاحبها. كما لقاضي التحقيق أن يطلع على البرقيات والرسائل ويحتفظ بما يراه منها ضروريا لإظهار الحقيقة أو بما يكون أمر اطلاع الغير عليه ضارا بالتحقيق. لا يحق له إفشاء مضمون أي برقية أو رسالة مضبوطة دون موافقة صاحب العلاقة.

وقد اولى القانون اهتماما خاصا في اصول تفتيش مكاتب المحامين اذ لحظ قانون أصول المحاكمات الجزائية أحكاما خاصة ترعى تفتيش مكاتب المحامين. وبالفعل، فان القانون ينص على أنه لا يحق لقاضي التحقيق، ما خلا الجريمة المشهودة، عند ملاحقته محامياً، أن يفتش مكتبه إلا بعد أن يعلم نقيب المحامين بالأمر، على أن لا يخرق أثناء تفتيشه سر المهنة. ويمكن للنقيب أو من ينتدبه أن يحضر أعمال التفتيش. كما لا يجوز لقاضي التحقيق أن يطلع على الرسائل المتبادلة بين المدعى عليه وبين وكيله المحامي.

ثانيا: حماية سرية الاتصالات والمراسلات وواقع التنصت

تأتي اشكالية التنصت التي تقوم به الحكومات والادارات المعنية لتأخذ حيزا كبيرا من النقاش، كون التنصت يندرج ضمن مسألة احترام الحياة الخاصة المحمية في الدستور ان لناحية حرمة المنزل او مبدأ سرية المراسلات او اي وجه من وجوه الحياة الخاصة. تبرر الدول التنصت بضرورة حماية امن الدولة الداخلي في وجه تنامي الارهاب والجرائم والخطر الخارجي في وجه محاولات التجسس وخرق امن الدولة. يسمح القانون اللبناني وتحديدا اصول المحاكمات الجزائية لقاضي التحقيق بالتنصت القضائي بغية اجلاء الحقيقة. الا ان ذلك يأتي ضمن حدود وهي "في المواد الجنائية والجنحية، شرط ان تكون العقوبة مساوية او متجاوزة لاربعة شهور حبس". على ان لا تتجاوز مدة التنصت الاربعة اشهر يمكن تمديدها مرة واحدة وان تكون موضوع محضر رسمي وان يتم اتلاف التسجيلات عند انقضاء مهلة الادعاء. كما ان المادة ١٧٤ من قانون المخدرات والمؤثرات العقلية والسلائف رقم ١٩٩٨/٦٧٣، نصت على أنه: للضابطة العدلية، بموافقة النيابة العامة، أن تضع تحت المراقبة أو التنصت خطوط الهاتف التي يستعملها أشخاص تتوافر

دلائل جدية تفيد اشتراكهم في إحدى جرائم المخدرات. لكنه لا يمكن اعتبار المكالمات التي حصل عليها بهذه الطريقة كإقرار، بل يستفاد منها في رصد تحركات الجناة وحسب والاستفادة من ذلك لكشف الجريمة.

اما الاطار القانوني الاكثر ردا على موضوع حماية الخصوصية فهو قانون التنصت رقم ٩٩/١٤٠ الذي يهدف الى صون الحق بسرية المخابرات التي تجرى بواسطة اية وسيلة من وسائل الاتصال. وتستعرض الاسباب الموجبة لهذا القانون سبب اقراره في وقت تسود الحياة السياسية اللبنانية منذ سنوات طويلة، مخاوف جدية من وجود تنصت سياسي او غير سياسي على المخابرات الهاتفية. ولما كانت هذه المخاوف ترتكز الى وقائع شهدتها البلاد في غير عهد من العهود، وادت في بعض الحالات الى اثارة اللغط حول بعض وجوه الممارسة الديموقراطية في لبنان. ولما كانت المحافظة على سرية المخابرات يشكل حقا من حقوق الانسان الاساسية التي ينص الدستور على احترامها. وان التعرض لهذا الحق يشكل استثناء لهذه القاعدة ولا يجوز ان يتم الا وفقا لاصول واضحة وفي حالات محددة ينص عليها القانون. ولما كان العهد الدولي الخاص بالحقوق المدنية والسياسية والاعلان العالمي لحقوق الانسان ينص في المادتين 12 و16 على عدم جواز التدخل بشكل تعسفي او غير قانوني في خصوصيات احد وفي حياته الخاصة او السرية او مسكنه او مراسلاته او على حساب سمعته وشرفه. وبما ان القانون الحالي لا يتضمن احكاما تحدد بشكل صريح ومفصل الحالات التي يجوز فيها اللجوء الى التدبير الاستثنائي القاضي باعتراض المخابرات الهاتفية. لذلك تم اعداد هذا القانون الذي يؤكد بأن مبدأ سرية المخابرات مصون بموجب القانون وانه لا يجوز التعرض له الا بموجب نص صريح يحدد اصول وشروط التعرض لسرية المخابرات التي تتم بأية وسيلة من وسائل الاتصال (الاتصالات عبر الاجهزة الثابتة او الخليوية او الفاكس او البريد الالكتروني...). كما يحدد القانون بصورة صريحة وواضحة الحالات التي يجوز فيها اللجوء إلى هذا التدابير ويفرق فيما بين:

أ- الاعتراض بموجب قرار قضائي:

يمنح القانون كلا من النائب العام لدى محكمة التمييز وقاضي التحقيق الاول في كل محافظة بموافقة وزير العدل ورئيس مجلس الوزراء صلاحية اتخاذ قرار يقضي باعتراض المخابرات، على ان يتناول هذا الاجراء الاستثنائي الشخص المظنون فيه بأنه فاعل او متدخل او شريك في جريمة معاقب عليها بالحرمان من الحرية لمدة لا تقل عن سنة على ان يضم الى ملف التحقيق فقط المعلومات المتعلقة بالجريمة.

ب- الاعتراض بموجب قرار اداري:

يمنح القانون كلا من وزيري الدفاع والداخلية بموافقة رئيس مجلس الوزراء صلاحية اتخاذ قرار يقضي باعتراض المخابرات بهدف جمع معلومات تتعلق بمحاربة الجرائم الواقعة على امن الدولة او الإرهاب او الجريمة المنظمة. يتم، في هذه الحالة، رصد المخابرات من قبل الاجهزة الامنية او الادارية التي يحددها الوزير في قراره، على ان تنظم هذه الاجهزة محضرا يتضمن فقط المعلومات التي تناولتها المخابرة المعترضة والتي لها علاقة بالموضوع سبب هذا الاجراء. كما ان القانون ينشئ هيئة مستقلة، مؤلفة من قضاة، تناط بها صلاحية التثبت من ان الاجراءات المتعلقة باعتراض المخابرات بناء على قرار اداري، تمت وفقا لاحكام القانون. وبما ان ضبط الاعتراض غير القانوني للمخابرات يتطلب وضع نصوص تعاقب على مثل هذه الافعال. لذلك، يلحظ القانون بأن اية مخالفة لهذه الجهة تشكل جنحة، تسري عليها مهلة مرور الزمن من تاريخ اكتشافها على ان لا يحول ترك الموظف او الاجير لوظيفته دون الملاحقة وان المشروع ينيط بالمحاكم العدلية وحدها صلاحية النظر في هذه الجرائم. [18]

يعتبر التنصت اذا اعتداء على الحريات الشخصية لاسيما الحياة الخاصة وسريتها. غير ان التنصت على المخابرات يؤمن للسلطات الامنية والقضائية أداة مهمة للكشف عن الاعمال الجرمية ودرء خطر المؤامرات

[18] http://www.legallaw.ul.edu.lb/Law.aspx?lawId=198664

على الدولة والمخططات الإرهابية التي تهدد امن المجتمع. وهنا تبرز مصلحتين يجب تأمين التوازن بينهما: المصلحة الفردية بحماية حرية شخصية والمصلحة الامنية الوطنية القومية.

وهذا ما أكده قرار المجلس الدستوري رقم ٩٩/٢ في معرض تعليله قبول الطعن المقدم في دستورية المواد ١٥ و١٦ من القانون رقم ١٤٠، حيث فسر القرار ان "هذا القانون يتناول بالتنظيم ويتعرض للحرية الفردية ويجيز التدخل في الحياة الخاصة للفرد من خلال الاجهزة بالتنصت او المراقبة او اعتراض المخابرات، من اجل ملاحقة الجرائم وجمع المعلومات لمكافحة الإرهاب والجرائم الواقعة على امن الدولة والجرائم المنظمة، ويضع بالتالي قيودا على ممارسة الحرية الفردية." وقد اعتبر القرار ان "الحرية الفردية هي حق من الحقوق الاساسية التي يحميها الدستور، ويتفرع عنها حرية التنقل، وحرية ابداء الرأي، وحرية المراسلات، وحرمة المنزل، واحترام الحياة الخاصة، وهذه الحريات صانها الدستور وجعلها في حماية القانون، وقد جاء النص عليها في الفصل الثاني منه،ولا سيما في المادة الثامنة)الحرية الشخصية) وفي المادة الثالثة عشرة (حرية ابداء الرأي قولا وكتابة) (وفي المادة 41 حرمة المنزل). وبما انه اذا كان الدستور ينيط بالمشترع حق وضع القواعد العامة التي توفر الضمانات الاساسية للحقوق وللحريات التي ينص عليها لكي يتمكن الافراد من ممارسة هذه الحريات، فانه يبقى للمشترع، ان يعمل على التوفيق والمواءمة بين احترام هذه الحريات من جهة والحفاظ على النظام العام من جهة ثانية الذي يجيز تقييد الحرية الفردية من اجل ملاحقة مرتكبي الجرائم والحفاظ على سلامة المواطنين وامنهم وحماية ممتلكاتهم، والذي بدونه لا يمكن تأمين ممارسة هذه الحريات، على ان يحيط ممارسة هذه الحريات بالضمانات الكافية." [19]

ان قانون صون الحق بسرية المخابرات التي تجري باية وسيلة من وسائل الاتصال قد نص في مادته الأولى على أن «الحق في سرية التخابر الجاري داخلياً وخارجياً من وسائل الاتصال السلكية أو اللاسلكية (الأجهزة

---

[19] قرار المجلس الدستوري ٩٩/٢، http://www.cc.gov.lb/ar/node/2577

الهاتفية الثابتة، والأجهزة المنقولة بجميع أنواعها بما فيها الخلوي، والفاكس، والبريد الإلكتروني..) مصون وفي حمى القانون،ولا يخضع لأي نوع من أنواع التنصت أو المراقبة أو الاعتراض أو الإفشاء، إلا في الحالات التي ينص عليها هذا القانون وبواسطة الوسائل التي يحددها ويحدد أصولها». كما نظّم هذا القانون أصول اعتراض المخابرات بناء على قرار قضائي وبناءً على قرار إداري، وحدد عقوبة التنصت غير الشرعي، وأنشأ هيئة مستقلة للتثبت من قانونية الاجراءات المتعلقة باعتراض المخابرات بناء على قرار إداري.

التنصت القضائي هو اجراء يتخذ بطلب صريح صادر عن سلطة قضائية مختصة،وهو يهدف الى التحري عن الجرائم المرتكبة والتثبت من هوية فاعليها والمشتركين فيها. وقد نصت المادة 2 من القانون اللبناني رقم ١٤٠ على أنه «في حالات الضرورة القصوى، لقاضي التحقيق الأول في كل محافظة إما عفواً أو بناءً على طلب خطي من القاضي المكلف التحقيق، أن يقرر إعتراض المخابرات التي تجري بواسطة أي من وسائل الاتصال المبيّنة في المادة الأولى من هذا القانون، وذلك في كل ملاحقة بجرم يعاقب عليه بالحرمان من الحرية لمدة لا تقل عن سنة يكون القرار خطياً ومعللاً،ولا يقبل أي طريق من طرق الطعن".

اي ان التنصت يجب ان يحصل فقط بناء على طلب قاضي التحقيق المختص ويكون كل تنصت تقوم به الضابطة العدلية مخالفا للقانون. كما حدّد القانون شروط التنصت القضائي وإجراءاته، فنصت المادة 3 منه على أنه "يحدد القاضي بالاعتراض وسيلة الاتصال التي يتناولها الاجراء والجرم موضوع الملاحقة أو التحقيق، والمدة التي تتم خلالها عملية الاعتراض، على ألا تتجاوز هذه المدة الشهرين،وعلى أن لا تكون قابلة للتمديد إلا وفق الأصول والشروط عينها". ونصت المادة ٤ على أنه "يجري اعتراض المخابرات وتسجيلها ووضع محضر مضمونها من قبل موظف الضابطة العدلية المكلف وفقاً للأصول، وذلك تحت سلطة القاضي الصادر عنه القرار ورقابته وإشرافه". ويتوجب على جميع العاملين لدى الجهات المعنية بموضوع وسائل الاتصال في القطاعين العام والخاص المعاونة في تنفيذ القرار القاضي بالاعتراض (المادة

٥)وينظم القاضي الصادر عنه القرار أو موظف الضابطة العدلية المكلف، محضراً بعملية الاعتراض يتضمن تاريخ وتوقيت بدء الاعتراض وانتهائه وتسجيله. كما ينظم محضراً يتضمن المعلومات ذات العلاقة بالموضوع. ويوضع التسجيل في غلاف يقفل ويختم بختم القاضي المختص وفقًا للأصول (المادة ٦). ويتلف التسجيل بناءً على قرار النائب العام لدى محكمة التمييز بعد انقضاء مهلة مرور الزمن على دعوى الحق العام، وينظم محضر بعملية إتلاف التسجيل (المادة ٧).

اما التنصت الاداري اي الذي تجريه السلطة الإدارية أو السياسية بهدف جمع المعلومات المتعلقة بالأمن الوطني ودرء خطر الإرهاب والتجسس وكل خطر يهدد الدولة والمجتمع، فقد حددته المادة ٩ من قانون التنصت رقم ١٤٠ باطار ضيق: "لكل من وزير الدفاع الوطني ووزير الداخلية ان يجيز اعتراض المخابرات بموجب قرار خطي معلل وبعد موافقة رئيس مجلس الوزراء, وذلك في سبيل جمع معلومات ترمي الى مكافحة الارهاب, والجرائم الواقعة على امن الدولة, والجرائم المنظمة. يحدد القرار وسيلة الاتصال موضوع الاجراء, والمعلومات التي يقتضي ضبطها, والمدة التي تتم خلالها عملية الاعتراض , على ان لا تتجاوز هذه المدة الشهرين, وعلى ان لا تكون قابلة للتمديد الا وفق الاصول والشروط عينها." على ان "يتلف التسجيل بعد انقضاء ثلاثة اشهر على تنظيم محضر المعلومات ما لم تقرر السلطة الآمرة بالاعتراض الاحتفاظ به لمدة مماثلة وفق الاصول والشروط ذاتها. ينظم محضر بعملية اتلاف التسجيل"، حسب المادة ١٢.

وتضيف المادة ١٣ ان "يمسك لدى كل من رئاسة مجلس الوزراء ووزارتي الدفاع الوطني والداخلية سجل تدون فيه كل عملية تجري بناء على قرار اداري, لا سيما تاريخ بدئها وانتهائها."

يشكل هذا النوع من التنصت الاداري مخالفة لحقوق الانسان والاتفاقات الدولية التي تعنى بحماية الخصوصية والحق بالحياة الخاصة لذا يأتي فقط في أطر استثنائية تتطلب موافقة رئيس مجلس الوزراء وبقرار معلل تحدد فيه تفاصيل العملية ومدة التنصت وانتهائه. اذ ان المس بحرية اساسية ممنوع في القاعدة

الا ضمن اطر ضيقة كتلك التي حددها قانون التنصت رقم ١٤٠ او عند اعلان حالة الطوارئ التي تستدعي حينها مجموعة تدابير تمس بالحريات الاساسية ومنها مراقبة النقل والمواصلات والاتصالات ولكن طبعا بمراسيم تتخذ في مجلس الوزراء وفق الآليات القانونية لاعلان حالة الطوارئ. فيشكل اذا التنصت الاداري الاستثناء وفي حالات ضيقة ومحصورة.

ومن حسنات القانون ١٤٠ انه اوجد آليات للرقابة على قرار التنصت الإداري فنصت المادة ١٦ على أنه "تنشأ هيئة مستقلة من الرئيس الأول لمحكمة التمييز ورئيس مجلس شورى الدولة ورئيس ديوان المحاسبة، تناط بها صلاحية التثبت من قانونية الاجراءات المتعلقة باعتراض المخابرات المتخذة بناءً على قرار إداري، ويترأس الهيئة القاضي الأعلى درجة. تبلغ الهيئة قرارات اعتراض المخابرات المتخذة بموجب قرار إداري خلال ٤٨ ساعة من صدورها. ويعود للهيئة، خلال مهلة سبعة أيام من تاريخ التبلغ، النظر في قانونية الاعتراض، وعند الضرورة إبلاغ رأيها بشأنه الى كل من رئيس مجلس الوزراء والوزير المختص. ويعود لها النظر في قانونية الاعتراض بناءً على مراجعة كل ذي مصلحة وفق الأصول ذاتها وذلك خلال سبعة ايام من تاريخ تقديم المراجعة. ويكون للهيئة أو لمن تنتدبه من أعضائها أوسع الصلاحيات لإجراء التحقيقات اللازمة مع الجهة الأمنية والإدارية والفنية المختصة ومع مؤسسات القطاع الخاص المعنية بموضوع وسائل الاتصال، ولها الحق في إجراء الكشف الحسي والاستعانة بمن تشاء من أهل الخبرة والاطلاع على المعدات والمستندات اللازمة مهما كانت درجة سريتها. وتضع الهيئة تقريراً سنوياً يتضمن بياناً بخلاصة أعمالها وباقتراحاتها، يرفع الى كل من رئيس الجمهورية ورئيس مجلس النواب ورئيس مجلس الوزراء ويحدد نظام عمل الهيئة بمرسوم يتخذ في مجلس الوزراء بناءً على اقتراح رئيس مجلس الوزراء. وتنحصر مهمة التنصت بوزارة الداخلية."

وقد صدر المرسوم رقم ٢٠٠٥/١٥٢٨١ الخاص بتنظيم عمل هذه الهيئة المستقلة. وتجدر الاشارة هنا أن المادة 16 أضيفت بموجب القانون رقم ١٩٩٩/١٥٨ بعد أن أبطل المجلس الدستوري في قراره تاريخ

٢٤/١١/١٩٩٩ المادة ١٦ القديمة التي كانت تنص على إنشاء هذه الهيئة من الرئيس الأول لمحكمة التمييز ورئيس مجلس شورى الدولة ونائبين يسميهما رئيس مجلس النواب، فاعتبر المجلس الدستوري أن اشتراك نواب في تشكيل الهيئة يشكل تدخلاً من قبلهم في أعمال السلطة التنفيذية بصورة مخالفة للدستور ولمبدأ الفصل بين السلطات. [20]

وفرضت المادة ١٧ عقوبة على مخالفة القانون "يعاقب بالحبس من سنة الى ثلاث سنوات وبالغرامة من خمسين الى مئة مليون ليرة لبنانية كل شخص يعترض اي مخابرة خلافا لاحكام هذا القانون. يعاقب بالعقوبة عينها كل من حرض او اشترك او تدخل في الجرم او استنسخ او احتفظ او افشى معلومات استحصل عليها لدى اعتراض المخابرات بناء على تكليف السلطات المختصة او اقدم على اعتراض المخابرات في غير الاماكن المحددة في قرار الاعتراض ."

بالرغم من ان هذا القانون يشكل حالة استثنائية لتضييقه حرية اساسية مكفولة في الدستور، وقد حد فعلا من امكانية التعرض للمخابرات الشخصية، لاسيما تلك التي تحصل بموجب قرارا اداري، اذ اشترط موافقة رئاسة مجلس الوزراء وحد اي اعتراض للمخابرات بمهلة زمنية قصيرة، الا انه بالممارسة فقد تمت مخالفة القانون بصورة متمادية وروتينية في ما عرف بملف تسليم داتا الاتصالات للاجهزة الامنية الذي سنعالجه في الفصل الثاني.

ثالثا: انتهاك الخصوصية اثناء تفتيش الهواتف والحواسيب

لا يوجد نص قانوني خاص يتعلق باصول تفتيش الهواتف والاطلاع على محتواها لاسيما ان قانون اصول المحاكمات الجزائية قد وضع قبل انتشار الهواتف الذكية تحديدا. هذه الهواتف باتت اليوم تحتوي على كل تفاصيل حياتنا الخاصة من محادثاتنا وصورنا الحميمة الى مراسلاتنا والكثير من المعلومات

---

[20] الدكتور نادر عبد العزيز شافي، دكتوراه دولة في الحقوق محام بالإستئناف، ورقة "بين احترام الحريات الشخصية ومراعاة مصلحة الدولة والأمن الوطني"، منشورة على موقع الجيش اللبناني، https://www.lebarmy.gov.lb/ar/content/بين-احترام-الحريات-الشخصية-ومراعاة-مصلحة-الدولة-والأمن-الوطني

الخاصة التي تتنقل معنا كيفما تحركنا. لا شك ان تفتيش الهواتف والحواسيب هو من اسهل الوسائل لجمع الادلة تستند اليها الضابطة العدلية والنيابات العامة غالبا دون ضوابط قانونية وبالتالي دون احترام لخصوصية المواطنين. ان الاطلاع على المحتويات الرقمية للهواتف والحواسيب يشكل دون شك تفتيشا بالمعنى القانوني اي اجراء من اجراءات التحقيق التي تهدف الى البحث عن ادلة جرمية او تدل على جرائم معينة وعلى مرتكبيها. ان عدم وجود نص يتعلق باصول تفتيشها لا يعني انها معفية من اية اصول، لاسيما لما تتضمنه من تعدي على الحرية الشخصية والحياة الخاصة.

وفي هذا الاطار يمكن الاشارة الى المادة 224 من قانون تنظيم قوى الامن الداخلي [21] انه "لا يجوز لرجال قوى الامن الداخلي في غير الحالات التي نص عنها القانون ان يزعجوا الناس في حريتهم الشخصية."

وتشير العديد من الجمعيات اللبنانية التي تعنى بالدفاع عن الحريات الشخصية لاسيما كل من المفكرة القانونية ومؤسسة مهارات وجمعية سمكس، فضلا عن منظمات دولية مثل "هيومان رايتس واتش" الى استمرار التعرض للحياة الخاصة لاسيما من قبل الاجهزة الامنية ان في التحقيقات من قبل الضابطة العدلية او على الحواجز على خلاف القواعد الموضوعة لاجراءات التفتيش المختلفة والتي تعتبر صارمة لجهة تحديد السلطات المخولة اجراءها والحالات والشروط المسموح فيها اتخاذ مثل هذه التدابير.

وفي قضية اعتبرتها المفكرة القانونية [22] الاولى من نوعها وذلك في معرض قرار صادر عن محكمة الاستئناف بابطال التعقبات بحق ثلاثة شبان اتهموا بممارسة علاقات مثلية، لعدم توفر الركن المادي للجريمة بمعزل عن قانونية الادلة، فقد ذهب المستشار القاضي ربيع معلوف ابعد من عدم توفر الركن المادي لبطلان التعقبات بل اعتبر ان انتزاع افادة احد الشبان تحت التعذيب وتفتيش هاتفه دون الحصول على اذن من قاضي التحقيق يجعل ضرورة ابطال كافة التحقيقات الاولية لمخالفتها الاصول. اذ أكّد القاضي معلوف

---

[21] http://www.legallaw.ul.edu.lb/LawView.aspx?opt=view&LawID=244510

[22] "مخالفة للقاضي ربيع معلوف: تفتيش الهواتف يتطلب اذنا من قاضي التحقيق"، المفكرة القانونية، https://www.legal-agenda.com/article.php?id=5541#_ftnref10

أنه يجب إبطال تفتيش الهواتف الذي قامت به الضابطة العدلية من دون إذن مسبق من قاضي التحقيق، وبالتالي عدم جواز استخدام المعلومات المستخرجة من الهاتف من أجل الإدانة. ان هذا الاجتهاد يشكل اساسا لملء فراغ قانوني ولمنع التعدي على الحياة الخاصة في عصرنا الرقمي الذي تستباح معه كل خصوصيتنا.

بدأ القاضي معلوف بالتأكيد على أن حق الانسان بحماية حياته الخاصة وخصوصية مراسلته هو من الحقوق الأساسية المحمية دستوريا وفي المواثيق الدولية،وأن المشترع اللبناني جسد هذه الحماية عبر وضع شروط قانونية توفر ضمانات أساسية لخصوصية المراسلات ضمن الموازنة ما بين احترام هذه الخصوصية والحفاظ على النظام العام. بالفعل، يمنع هذا الحق الدستوري التدخل التعسفي في الحياة الخاصةوالمراسلات. وهو ما أكد عليه المجلس الدستوري في معرض مراجعته للقانون رقم 140/1999 المتعلق بصون الحق بسرية المخابرات حيث اعتبر أن الاطلاع على المراسلات يشكل تعرضاً للحرية الفردية وتدخلاً في الحياة الخاصة المحمية دستورياً. فضلا عن أن التشريع والاجتهاد اللبنانيان يقران بمبدأ سرية المراسلات كمبدأ قانوني عام. ويستتبع هذه الخلاصة أن أي تعرّض لهذا الحق مثل تفتيش الهواتف يخضع لنظام قانوني يتضمن عدداً من الضمانات، وذلك استناداً إلى المبادئ القانونية العامة التي تنظم القيود على الحقوق والحريات الدستورية. ومن أهم هذه الضمانات أن يكون التعرّض منصوصاً عليه صراحة في القانون، وألا يتم إلا في حالة الضرورة ومن دون تجاوز مبدأ التناسب بين خطورة التعرّض وأهمية الغاية المراد تحقيقها من خلاله.

تبعاً لذلك،رأى القاضي معلوف أن إجراء تفتيش الهواتف يخضع للضمانات التي وضعها المشرّع اللبناني في القانون رقم ١٤٠/١٩٩٩ المتعلق بصون سرية المخابرات، معتبراً أن هذه الشروط تمنع التجاوزات خلال التحقيقات الجزائية وتضمن التوازن بين احترام الخصوصية والحفاظ على النظام العام. وبهذا يكون حسم موقفه حول وجوب تطبيق أصول تفتيش المراسلات على تفتيش الهواتف، أسوة باجتهادات دول أخرى

وضعت ضوابط قضائية في هذا الخصوص، لا سيما الولايات المتحدة الأميركية (رايلي ضد كاليفورنيا، ٢٠١٤).

هذا القانون يؤكّد على مبدأ سرية المراسلات وينظّم آلية اعتراضها والاطلاع عليها بشكل صارم، وذلك لأن "التعرض لهذا الحق يشكل استثناء لهذه القاعدة ولا يجوز أن يتم إلا وفقا لأصول واضحة وفي حالات محددة ينص عليها القانون ."ويتضمن القانون آليتين مختلفتين لاعتراض المخابرات: الأولى بموجب قرار قضائي في إطار التحقيقات الجزائية، والثانية بموجب قرار إداري صادر عن وزيري الدفاع والداخلية بموافقة مجلس الوزراء بهدف جمع المعلومات عن الجرائم الخطيرة، وهي الآلية المستخدمة من أجل منح الأجهزة الأمنية داتا الاتصالات.

والشروط الأساسية التي فرضها هذا القانون على القرار القضائي باعتراض المخابرات والتي يجب أن يخضع لها أيضاً قرار الاطلاع على محتوى الهواتف، هي الآتية:

- أن المرجع لاتخاذ القرار هو قاضي التحقيق، وهذا ما تؤكد عليه أيضاً المادة ١٠٢ من أصول المحاكمات الجزائية التي تحصر إمكانية الاطلاع على البرقيات والرسائل بقاضي التحقيق وحده. ويستتبع ذلك أمران: الأول أن تفتيش الهواتف يتطلب إذناً قضائياً ولا يدخل ضمن صلاحيات الضابطة العدلية التي لها صلاحية تفتيش الأشخاص في بعض الحالات المحددة. والثاني، أن الجهة القضائية التي يحق لها الاطلاع على محتوى الهواتف ليست النيابة العامة، التي هي خصم في الدعوى الجزائية وتخضع للهرمية والتسلسلية، بل قضاة التحقيق الذين يتمتعون بضمانات الاستقلالية والحيادية.
- أن القرار محصور في حالات الضرورة القصوى، بمعنى أنه على قاضي التحقيق التثبت من وجود ضرورة تتعلق بحماية النظام العام أو غايات التحقيق من أجل اتخاذ قراراً بالاطلاع على محتوى هواتف المشتبه فيهم.

- أن القرار محصور في سياق ملاحقة جرم يعاقب عليه القانون بالحرمان من الحرية لمدة لا تقل عن سنة، أي أن تكون الجريمة التي يتم التحقيق بها بدرجة من الخطورة لتبرير التعرّض للحياة الخاصة.
- أن القرار يجب أن يكون خطياً ومعللاً، وهو شرط شكلي يضمن الالتزام بجميع الشروط المذكورة أعلاه. فشرط التعليل الخطي لأسباب تفتيش الهواتف هو أمر ضروري للحد من التعرّض للحياة الخاصة كونه شكلاً من أشكال الرقابة الذاتية للقضاة وضمانة لاستخدام التفتيش كتدبير استثنائي في حالات الضرورة القصوى فقط.

هذا واستكمل القاضي معلوف اجتهاده لناحية اعتبار تفتيش الهواتف بشكل مخالف للاصول باطلا اذ يقتضي "إبطال كافة التحقيقات الأولية المرتكزة على المعلومات الواردة على هاتف المستأنف"، كما اضاف سندين قانونيين لذلك: مخالفة صيغة جوهرية وهي اغفال ضمانة دستورية "حماية خصوصية الأفراد المصانة دستورياً من أي تعسف خلال مرحلة التحقيق"،والقياس على النص القانوني المتعّلق بتفتيش المنزل لامكانية ابطال التفتيش الذ لا يكون مطابقا للاصول القانونية. وبما أن المشترع أكّد صراحة على إبطال تفتيش الأشخاص والمنازل في حال لم تستحصل الضابطة العدلية على إذن من النيابة العامة، فإنه يستنتج قياساً أنه يجوز إبطال تفتيشها للهواتف في حال لم تستحصل على إذن من المرجع القضائي المختص الذي هو قاضي التحقيق وفقًا لقانون سرية المخابرات.

وفي العام ٢٠٠٥ صدر المرسوم رقم ١٥٢٨٠ "تحديد اماكن واصول اعتراض المخابرات"[23]. وقد أنشأ هذا المرسوم جهازا خاصا لاعتراض وتسجيل المخابرات الهاتفية وذلك في المبنى المركزي لوزارة الاتصالات في بيروت. ينشأ الجهاز لدى وزارة الداخلية ويرتبط مباشرة بالوزير، مهمته القيام بعملية اعتراض المخابرات الهاتفية بناء على قرار إداري وتسجيلها وفقا لأحكام هذا المرسوم.و يتألف من:

---

[23] مرسوم رقم ١٥٢٨٠/٢٠٠ http://www.legiliban.ul.edu.lb/LawView.aspx?opt=view&LawID=211716

. ضابط قائد على الأقل يتم اختياره من قبل وزارة الداخلية والبلديات.

- ضابط قائد على الأقل يتم اختياره من قبل وزارة الدفاع الوطني.

- موظف مختص من الفئة الثانية يتم اختياره من قبل وزارة الاتصالات.

وهو يقوم بتنفيذ قرارات الاعتراض الادارية الصادرة عن وزير الدفاع او وزير الداخلية وينظم محضرا بعملية الاعتراض يتضمن تاريخ وتوقيت بدء الاعتراض وانتهائه وتسجيله كما يتضمن المعلومات ذات العلاقة بالموضوع. اما قرارات الاعتراض القضائية فتبلغ الى وزير الداخلية لتنفيذها فورا.

ولطالما شكل هذا الجهاز مادة للسجال السياسي على حساب نقاش مفتوح وشفاف حول مدى احترامه لخصوصية المواطنين ومدى تقيده بالاصول والآليات المنصوص عنها في قانون التنصت.[24] وليس هناك اية تقارير صادرة عن وزارة الداخلية او وزارة الاتصالات حول قدرة وعمل هذا الجهاز والعمليات التي يجريها. واوردت جريدة الاخبار انه يتيح مراقبة مكالمات 360 هاتفًا خلويًا في وقت واحد، فضلاً عن تعقب 48 ألف هاتف خلوي في اليوم الواحد، فضلاً عن تسجيل كل الرسائل النصية (SMS) وحركة الاتصالات. وليس هناك وضوح حول مدى إمكانية المركز مراقبة الشبكة الثابتة وشبكة الإنترنت.

رابعا: انتهاك الخصوصية في تطبيقات التتبع الالكتروني لمكافحة الكورونا

عملت العديد من الحكومات حول العالم على تطوير تطبيقات تتبع الكتروني لمكافحة انتشار وباء كورونا عبر تقنيات تتبع عبر GPS سواء لحصر انتشار الوباء او لتقرير رفع الحظر تدريجيا. لكن هذه التطبيقات تطلب الكثير من الاذونات للدخول الى بيانات الهاتف مثل الملفات الصوتية والفيديوهات وقائمة الاتصالات وليس فقط الموقع الجغرافي وتقنية بلوتوث لتحديد الاشخاص الذين خالطوا المصاب. وقد أعلت المنظمات الحقوقية الصوت حول العالم إزاء هذه التطبيقات. فقد اعتبرت منظمة الخصوصية الدولية ان موجة المراقبة الناتجة عن القوانين والصلاحيات الموسعة والتكنولوجيا التي يتم استخدامها

---

[24] https://al-akhbar.com/Politics/143787

لمكافحة انتشار الوباء حول العالم تشكل خوفا غير مسبوق للحريات الانسانية. بعض التدابير تهدف فعلا الى الحفاظ على الصحة العامة الا ان بعضها الاخر يقترب الى قبضة اكبر على الحريات. كما دعت المنظمات الدولية الحكومات،رغم الجائحة، الى العمل على اختيار التدابير الاكثر ملاءمة مع المشروعية وبناء الثقة العامة واحترام رفاه الناس وذلك عبر جعل تأمين الحماية للمواطنين اولوية عوضا عن مزيد من أدوات التحكم التي ترعى مصالحها. [25] اذ اعتبرت المنظمات الحقوقية ان الحكومات والشركات حول العالم اتجهوا الى تقنيات مراقبة غازية للخصوصية لمواجهة الازمة. هذه التدابير تراوحت بين استخدام مخبرين، شرطة مراقبة، نشر اسماء المصابين الى تطبيقات التتبع الالكتروني. وقد شددت المنظمات على ضرورة ان تكون التدابير المتخذة استجابة لمكافحة انتشار الفيروس قانونية، ضرورية، متناسبة، مربوطة بزمن ومبررة بمشروعية اهداف الصحة العامة. كما ان منظمة الصحة العالمية اشارت الى ان هذه التطبيقات لا تعوّض التعقّب اليدوي التي تقوم به السلطات الصحية لاسيما انه تقنيا يحصل انتشار الفيروس بين الأشخاص الذين يتقاربون لمسافة أقل من متر عبر رذاذ عطاسهم ويمكن للفيروس أن ينتقل عبر لمس الأسطح أو في الأماكن المزدحمة المغلقة. كل ذلك يعزز التشكيك بفعالية هذه التطبيقات وفاعلية بيانات الموقع الجغرافي في تتبع المرض ودقتها في تعريف المُخالطين، خصوصاً بمرض ينتقل عبر حبيبات الرذاذ. خاصة انه لا يمكن توفير بيانات دقيقة عن تقارب الاشخاص من بعضهم البعض عبر بيانات موقع أبراج الاتصالات، نظرًا لتراوح محيط المساحة التي تغطيها أبراج الاتصالات بين ٥٠ إلى ١٠٠ متر. قد تمنح بيانات الموقع (GPS) التي تحصل عليها تطبيقات التتبع عبر الهاتف دقة أكبر بمحيط خمسة أمتار إذا تواجد الشخص في أماكن خارجية، لكن الـ GPS لن يخبرك عن مدى تقارب الأفراد في مكان داخلي متعدد الطوابق. كذلك، وجهت الانتقادات للتطبيقات التي تعتمد على تقنية البلوتوث لقياس التقارب بدلًا من الموقع الجغرافي. إذ تختلف المساحة التي تغطيها تقنية البلوتوث بحسب

[25] بيان المنظمات الحقوقية للحكومات https://privacyinternational.org/press-release/3581/civil-society-sound-alarm-over-unprecedented-global-wave-surveillance-fight

الهواتف الذكية. قد يكون محيط المساحة التي تغطيها تقنية البلوتوث أصغر من GPS إلا أنها قد تعطي تنبيهات كاذبة عن التقارب نظرًا لتمكنها من اختراق الجدار. فإذا أصيب جارك الذي يسكن فوقك أو بجانبك، قد يعطيك التطبيق تنبيهاً كاذباً عن احتمالية مخالطتك له حتى وإن لم تره. [26] اما في لبنان، فقد وثقت مؤسسة مهارات في تقريرها عن "تطبيقات التتبع الالكتروني والخصوصية" ان وزارة الصحة اللبنانية اطلقت تطبيقين على متجر التطبيقات، الاول يحمل اسم وزارة الصحة العامة (Ministry of Public Health) يوفر للمستخدمين أسعار الأدوية ومواقع الصيدليات كما أضيف إليه حديثًا قسم عن أخبار فيروس كورونا وتشخيص المرض لدى المواطنين. والتطبيق الثاني باسم "اي هيلث ليبانون" (eHealth Lebanon) يساعد المواطنين في طلب مساعدات من الوزارة عبر تعبئة طلبات مخصصة. وأكدت منظمة "سميكس "التي تعنى بالحقوق الرقمية عبر موقعها ان التطبيقين يتطلبان الكثير من الأذونات غير الضرورية، مثل الوصول إلى الكاميرا والميكروفون والموقع الجغرافي، وبعض الأذونات الضرورية لتشغيل خدمات التطبيقات، مثل طلب الوصول إلى مكان تخزين المعلومات لكي يتمكن مستخدمو التطبيق من تحميل مستندات على التطبيق. يسمح تفعيل كل تلك الأذونات للتطبيقات بجمع معلومات شخصية عن المستخدمين ويفتح الباب أمام المهاجمين للحصول على تلك البيانات بسهولة أو الاستفادة من الأذونات للوصول إلى أجهزة المستخدمين بحد ذاتها. كما ان هذه التطبيقات لا تتضمن سياسات خصوصية واضحة.

هذا اضافة الى اطلاق تطبيق "معًا" للتتبع الالكتروني الذي اطلقه وزير الصحة حمد حسن في ١٦ تموز ٢٠٢٠ .[27] يعتمد التطبيق على تقنية بلوتوث بحسب ابو مراد وتم إطلاقه بالتعاون مع "الجامعة الاميركية

[26] تقرير مهارات ماغازين حول تقنيات التتبع الالكتروني والخصوصية في البلدان العربية:
http://magazine.maharat-news.com/coronaappprivacy2

[27] https://www.almarkazia.com/ar/news/show/235133/حسن-يطلق-التطبيق-الإلكتروني-معا-ضد-كورونا-لتتبع-ا

في بيروت.(AUB) "وتقول مديرة البرنامج الوطني للصحة الإلكترونية في وزارة الصحة العامة لينا ابو مراد ممثلة وزارة الصحة ان "التطبيق اللبناني يراعي خصوصية المستخدمين، حيث أن البيانات الناتجة عن تطبيق "معا "ستكون مخزنة على هاتف المستخدم وفي حال أبلغ عن إصابته تُحمّل البيانات إلى سيرفرات (خوادم) تابعة لوزارة الصحة،ولا يوجد إمكانية لأي جهات الوصول إلى هذه المعلومات سوى الوزارة. كما ان التطبيق لا يطلب أسماء المستخدمين، إنما فقطرقم الهاتف للتواصل مع الشخص في حال الاصابة أو مخالطة مصاب بالفيروس". هذا النقاش حول الخصوصية في هذه التطبيقات تمت مناقشته في المنتدى اللبناني لحوكمة الانترنت في جلسة عقدت في ٢٤ تموز ٢٠٢٠[28] ، نظمتها مؤسسة مهارات ومنظمة سمكس وأضاءت على الأطر القانونية المتوفرة وتوافقها مع المعايير الدولية، كما بحثت في توفر الشفافية أثناء تطوير أدوات الصحة العامة، إضافة إلى إدارة البيانات ومعالجتها وتخزينها، ودور جميع أصحاب المصلحة، وخاصة الثغرات الحمائية في منظومة القوانين اللبنانية لاسيما القانون رقم ٨١، المعاملات الالكترونية وحماية البيانات الشخصية. حيث اعتبرت القاضية هانية حلوة التي كانت قد شاركت في نقاشات صياغة هذا القانون ان الدولة اللبنانية يجب أن تكون خاضعة لموجبات قوانين حماية البيانات الشخصية. واكدت على ان هناك ثغرات عدة في قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، أبرزها عدم الاشارة الى موضوع الرضى وضرورة وجود هيئة ناظمة مستقلة للرقابة المسبقة على حماية البيانات لأن الرقابة اللاحقة للحماية لا تكفي. "هذه الهيئة التي لم يتضمنها القانون بسبب تباين وجهات النظر السياسية هي أكثر من ضرورية وفق كل معايير الحماية"، هذه كانت ابرز خلاصات هذه الجلسة.

ومن الواضح ان هناك تخبط بالتعاطي مع موضوع الخصوصية في لبنان وتفاوت بين الادارات وعدم تنسيق. بدا ذلك جليا في مذكرة وزارة الداخلية والبلديات المذكرة رقم ٧٦/أ.م [29] التي صدرت في ٢٧ تموز

[28] http://maharatfoundation.org/igflebanon24july

[29] www.interior.gov.lb/AdsDetails.aspx?ida=368

٢٠٢٠ وتتعلق بتعديل التدابير والإجراءات الوقائية لمواجهة وباء كورونا. وتضمن في "ثالثا "التدابير والاجراءات الوقائية الواجب تطبيقها في المرافئ الحدودية على جميع الوافدين الى لبنان وضمنها أ –اعتبارا من ٢٨ تموز تحميل التطبيق الخاص بوزارة الداخلية والبلديات لتتبع تحركاتهم. وقد اوضح رئيس وحدة التحليل والتخطيط والتنسيق في وزارة الداخلية الرائد طارق حسب الله في مقابلة لموقع مهارات نيوز [30] ان التطبيق هو في طور التطوير من قبل شركة أجنبية وهو يستخدم تقنية GPS وسيكون تنزيله الزاميا على ان تتوافر معلومات اكثر عن انتهاء العمل بالتطبيق الاسوع المقبل. ويهدف التطبيق حسب الرائد حسب الله الى تتبع الوافدين القادمين من الدول التي لديها نسب اصابات مرتفعة والتأكد من التزامهم الحجر. ولم يظهر ان هناك تفاصيل حول معايير الخصوصية التي سيتطلبها التطبيق.

خامسا: غياب الاطر الناظمة لعمل مزودي خدمات الانترنت

يصل مزودو خدمات الانترنت الذين نعتمد عليهم في لبنان لتوفير الاتصال بالانترنت الى الكثير من بياناتنا الحساسة من الروابط التي نزورها، موقعنا الجغرافي، بياناتنا وبريدنا الالكتروني ومعلومات بطاقاتنا الائتمانية حتى. تشكّل هيئة اوجيرو لخدمات الاتصال الثابتة والمملوكة للدولة، البنية التحتية الأساسية لجميع شبكات الاتصالات، بما في ذلك مشغلي شبكات الهاتف المحمول، ومقدمي خدمات البيانات (DSP)، ومقدمي خدمات الإنترنت (ISP) وغيرها. لا تتيح أوجيرو سياسة خصوصية ولا شروط استخدام على موقعها الإلكتروني، ولا توضح كيفية إدارتها لبيانات المستخدمين. يحقّ للمستخدمين معرفة كيف تتعامل أوجيرو ومقدّمو خدمات الإنترنت الآخرون مع بياناتهم وكيف تتصرّف بها. [31] هناك حوالي ١١٤ مزود خدمة انترنت في لبنان حسب المسح الذي اجرته منظمة سمكس، معظمها لا تنشر سياسات خصوصية واضحة تمكن المستخدمين من تحديد البيانات التي يتم جمعها من قبل الشركات وكيف يتعاملون مع هذه

[30] https://maharat-news.com/coronaappchecked

[31] تقرير منظمة سمكس حول "مقدمو خدمات الانترنت في لبنان يفتقرون الى الشفافية"، https://smex.org/ar/مقدّمو-خدمات-الإنترنت-في-لبنان-يفتقرو/

البيانات لجهة بيعها او مدة الاحتفاظ بها او محوها. ان الاطار الرقابي القانوني لمزودي خدمة الانترنت وقطاع الاتصالات عموما يتمثل في "الهيئة المنظمة للاتصالات" TRA وهي هيئة مستقّلة، جرى تأسيسها بهدف تحرير وتنظيم وتطوير سوق الاتصالات في لبنان. وفي أعقاب تأسيسها بموجب قانون الاتصالات رقم ٤٣١ لسنة ٢٠٠٢، باشرت الهيئة بالقيام بعملياتها إثر تعيين مجلس إدارتها في شهر شباط ٢٠٠٧. تكمن مهمّتها الأساسية في تعزيز المنافسة داخل قطاع الاتصالات، وحماية حقوق المستهلكين والشركات، من خلال الإجراءات المناسبة للتنظيم والتقرير. الهيئة مسؤولة عن إصدار التراخيص والأنظمة، وإدارة حّيز الترددات اللاسلكية ومخطّط الترقيم الكلي، ومراقبة السوق لرصد أي استغلال للقوة التسويقية الهامة والممارسات التي تناقض المنافسة، فضلاً عن اتخاذ الخطوات العلاجية عند اللزوم. غير أنه جرى تجميد عملها بقرار قضائي صادر عن مجلس شورى الدولة عام ٢٠٠٩ اعتبر فيها ان انشاءها وتنفيذها لصلاحياتها غير نافذ لحين استكمال قانون الاتصالات لجهة انشاء شركة ليبانتيليكوم. بالتالي يكون الاطار المولج بمراقبة عمل مزودي خدمات الانترنت لجهة احترام حقوق المستهلكين ومنها حقهم بالخصوصية غير مفعل.

سادسا: غياب حماية الحق بالسرية والهوية المغفلة على الانترنت

يستلزم الحق في الحياة الخاصة والحق في حرية التعبير حقًا آخر يعتبر نتيجة لهما، وهو الحق في "الهوية المغفلة"، أي عدم الكشف عن هوية المستخدم على الانترنت. ان الهوية المغفلة تتيح للأشخاص التعبير دون الكشف عن هويتهم الامر الذي قد يحميهم من الانتقام او الملاحقة الأمنية.

وقد اولى المقررون الخاصون للامم المتحدة اهتماما بحماية التشفير والهوية المغفلة في الاتصالات الرقمية لتوفير ضمانة اكبر لحق الافراد بالتعبير عن رأيهم. فقد كان هذا الموضوع اساسا للتقرير الاول الذي قدمه المقرر الخاص عن حرية الراي والتعبير دايفيد كاي لمجلس حقوق الانسان عام ٢٠١٥ [32]. برر كاي اهمية الموضوع نظرا لتحول العالم الى التعقب الشامل والهجومات الرقمية على الافراد والمجتمع المدني،

---

[32] https://www.ohchr.org/EN/NewsEvents/Pages/HRencryptionanonymityinadigitalage.aspx

فضلا عن الفئات المهمشة وما ينتج عن ذلك التعقب من توقيفات واعتداءات جسدية وحتى قتل. وشدد على اهمية ايلاء موضوع التشفير والهوية المغفلة كأساس لحرية التعبير في العالم الرقمي اذ يشكلان ادوات حماية رقمية ضرورية لممارسة الحق بالتعبير الحر. وتطرق ايضا في رسالته الى مجلس حقوق الانسان الى ان الدول تتذرع لمنع ادوات الخصوصية هذه بقدرتها على مكافحة الارهاب واحترام النظام العام. الا ان ذلك لا يجب ان يشكل حجة اذ انه تدبير غير متناسب ويعرض حرية اساسية للخطر. والقاعدة ان على الحكومات عندما تريد الوصول الى معلومات مشفرة او مغفلة عليها ان تطلب اذنا من القضاء. كما اوصى كاي بان الحكومات لا يمكن ان تطلب من الشركات الخاصة ان تعمل على برمجيات تقوض التشفير والاغفال لكي تعطي للحكومات الوصول. بل على الحكومات ان تحمي استخدام هذه الادوات كمسألة امن رقمي.

كذلك طالب المقرر الخاص عن الحق بالخصوصية في تقريره السنوي الاخير الذي قدمه في شباط ٢٠٢٠ الى مجلس حقوق الانسان [33] ، باحترام اخفاء الهوية والتشفير. وشدد في تقريره حول الخصوصية من منظور جندري، ان على الدول ان تضمن حماية شاملة للامن الرقمي بما في ذلك تعزيز ادوات الامن الرقمي وخدمات التشفير اذ ان وضع قيود على هذه الادوات يشكل خرقا للحق في الخصوصية، واذا ارادت الدول ان تضع قيودا فيجب ان تبقى على اساس كل حالة على حدة وان تكون معقولة وضرورية ومتناسبة والا تميز على اساس الجنس او اي عامل آخر. واعاد التذكير في تقريره ان كافة الدول يجب ان تعيد النظر في قوانين الجرائم السيبرانية والرقابة ومكافحة الارهاب لتتلاءم مع المعايير الدولية لحقوق الانسان التي تطبق على الحق بالخصوصية، حرية التعبير، حرية التجمع وحرية الجمعيات.

وقد وثقت مجلة مهارات في عدد خاص عن الامن الرقمي كيف تعاطت الدول حول العالم مع موضوع التشفير والهوية المغفلة. فقد فرضت العديد من الدول قيوداً لا مبرر لها على الحق في إخفاء الهوية على

[33] https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

الإنترنت. ففي كوريا الجنوبية، على سبيل المثال، يسمح القانون بالوصول إلى بيانات هوية العميل التي يحتفظ بها مزودو خدمات الاتصالات دون إذن، وهو ما استدعى اعتراض مجموعة من المدافعين عن الحقوق الرقمية أمام المحكمة الدستورية لكوريا. وفي عام 2017، شددت ألمانيا قوانين الأمن المتعلقة بتسجيل المستخدمين لدى شراء الخطوط الهاتفية (Sim Card). اما في روسيا، فقد اضطر مقدمو خدمات الانترنت الى الكشف عن هوية المستخدمين الخاضعين لتحقيق حكومي. وفي الصين، خضعت Apple لضغوط الحكومة لإزالة خدمات التشفير VPN من متجر التطبيقات الصيني الخاص بها بعد إصدار قانون لتقييد هذه البرامج على البنية التحتية لشبكة الدولة. [34] اما في الدول العربية فقد جرمت بعض الدول التشفير او استخدام هوية مغفلة على الانترنت بمجرد الكشف عن المستخدم الحقيقي. ومن هذه الدول مصر التي تجرم استخدام ادوات التشفير والامان الرقمي وكذلك كل من تونس والمغرب. اما في لبنان فليس هناك قوانين محددة تجرم التشفير او الهوية المغفلة بحد ذاتها.

المطلب الثاني: حماية الحق بالخصوصية وفق المعايير الدولية

أوضحت لجنة حقوق الانسان التابعة للامم المتحدة في تعليق عام على المادة ١٧ من العهد الدولي الخاص للحقوق المدنية والسياسية ان الحق في الخصوصية يشمل الحق في الحماية ضد كل تلك التدخلات والاعتداءات اكانت صادرة عن سلطات الدولة او من الاشخاص الطبيعيين او الاعتباريين.

ولكن لا يمنح هذا التعليق العام سوى توجيه بسيط عما يعنيه مصطلح "تعسفي" او "خصوصية". اذ ذكرت اللجنة ان التدخل يمكن ان يكون تعسفيا ومن ثم يجب ان تكون هذه التدخلات وفقا لاحكام واهداف واغراض العهد وان تكون معقولة في اي حال، وفي ظروف محددة. [35]

[34] http://magazine.maharat-news.com/anonimitydsi5

[35] التعليق العام رقم ١٦: الحق في احترام الخصوصية، والاسرة والمسكن والمراسلات وحماية الشرف والسمعة. (المادة ١٧)، اعتمد في ٤ آب ١٩٨٨، الفقرة ١.

اما الاتفاقية الاوروبية لحقوق الانسان فقد صاغت هذا الحق في مادتها الثامنة بشروط مختلفة عن العهد الدولي الخاص والاعلان العالمي لحقوق الانسان واتت على النحو التالي:

- لكل انسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته.
- لا يجوز للسلطة العامة ان تتعرض لممارسة هذا الحق الا وفقا للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الامن القومي وسلامة الجمهور او الرخاء الاقتصادي للمجتمع، او حفظ النظام العام ومنع الجريمة، او حماية الصحة العامة والآداب، او حماية حقوق الاخرين وحرياتهم.

اذا وضعت معايير واضحة لحماية الحق في الخصوصية: ١) وفقا للقانون، ٢) الضرورة في مجتمع ديمقراطي، و٣) حماية احدى المصالح المذكورة (الامن القومي وحفظ النظام العام ومنع الجريمة او حماية الصحة العامة والاداب او حقوق الاخرين وحرياتهم.

ان المبادئ الاكثر وضوحا عن كيفية تطبيق القانون الدولي لحقوق الانسان في البيئة الرقمية اليوم لاسيما في ضوء التغيرات في تكنولوجيا وتقنيات مراقبة الاتصالات، مراعاة للحق في الخصوصية، نجدها في تقرير "ضروري ومتناسب" الذي يضع ١٣ مبدأ دوليا على تطبيق حقوق الانسان على مراقبة الاتصالات. [36] وقد طور هذه المبادئ بطريقة تشاركية مجموعة من المؤسسات التي تعنى بالخصوصية وخبراء من حول العالم، ضمنهم "Access"، "Article 19"، "Electronic Frontiers Foundation"، " Reporters without borders"، "Privacy International"، "شبكة IFEX" وغيرهم. شارك اكثر من ٤٠ خبيرا في الخصوصية والامن في صياغة هذه المبادئ في اجتماع عقد في تشرين الاول ٢٠٢٠ في بروكسل، ثم خضع لاستشارات اوسع وتمت بلورة المسودة الاولى في ١٠ تموز ٢٠١٣ وتم اطلاقه رسميا في مجلس حقوق الانسان في الامم المتحدة في جنيف في ايلول ٢٠١٣. وبعد تبنيه من اكثر من ٤٠٠ منظمة حول العالم تم ادخال بعض التعديلات اللغوية الطفيفة عليه لتتم بلورة النسخة النهائية في ايار ٢٠١٤، على ان

[36] https://necessaryandproportionate.org/files/en_principles_2014.pdf

تزود هذه المبادئ مجموعات المجتمع المدني والدول والشركات وكافة اصحاب المصلحة باطار يمكن على اساسه تقييم قوانين المراقبة والتنصت والممارسات المرتبطة بانتهاك الخصوصية وما اذا كانت متلازمة مع حقوق الانسان.

وتمت صياغة هذه المبادئ على ان الخصوصية هي حق اساسي من حقوق الانسان وهي مركزية في الحفاظ على مجتمعات ديمقراطية. كما انها اساسية لممارسة حقوق اخرى مرتبطة بها مثل حرية التعبير وحرية التجمع وهي معترف بها في القانون الدولي لحقوق الانسان. ان تداخل مراقبة الاتصالات والتواصل مع الحق بالخصوصية يجعله مبررا فقط اذا اتى ضمن القانون وكان ضروريا يخدم هدفا مشروعا ومتناسبا مع الهدف المرجو.

ان مراقبة الاتصالات في البيئة العصرية يتخطى المراقبة والتنصت وجمع البيانات وتحليلها والوصول اليها والافعال المرتبطة بالمعلومات التي تعكس تواصل الافراد في الماضي والحاضر والمستقبل. بل تتضمن نشاطات ومعاملات وتفاعلات عبر وسائط الكترونية مثل محتوى الاتصالات وهوية الاطراف والتعقب الجغرافي ومعلومات مثل عناوين البروتوكولات الخاصة ووقت ومدة الاتصالات والادوات المستخدمة في الاتصال. هذا فضلا عما يسمى "الميتاداتا" وهي المعلومات التي لا تكون متوفرة للعامة بل لدى الشركات التي تحفظ الداتا وهي قد تحتوي على معلومات حساسة ترتبط بخصوصية الافراد اذ يمكن تحليلها لكشف سلوك الافراد واهتماماتهم وحالتهم الصحية وميولهم الجنسية وآرائهم السياسية وغيرها. هذه المعلومات تتطلب كذلك الحماية.

لذا ان تحديد ما اذا يمكن للحكومات ان تقوم بمراقبة الاتصالات آخذة بالاعتبار حماية المعلومات يجب ان يراعي المبادئ التالية:

1. المشروعية: ان اي قيد على حقوق الانسان يجب ان يكون بموجب القانون. على ان يكون القانون متاحا للعموم ومراعيا لمعايير الوضوح والدقة ما يضمن ان الافراد ملمون به ويفهمون تطبيقه. ونظرا

الى التطور التكنولوجي المتسارع، يجب اجراء مراجعات دورية تشاركية للقوانين التي تحد من حقوق الانسان.

2. الهدف المشروع: لا يمكن للقوانين ان تسمح بمراقبة الاتصالات من سلطات معينة الا لهدف مشروع يرتبط بمصلحة قانونية مهمة ضرورية في مجتمع ديمقراطي.ولا يجب لاي اجراء ان يطبق بطريقة تمييزية على اساس العرق او الجنس او اللغة او الدين او الرأي وغيرها من العناصر الشخصية.

3. الضرورة: ان قوانين المراقبة والممارسات المرتبطة بها يجب ان تكون محدودة فقط بما يمكن اثبات انه ضروري لتحقيق الهدف المشروع.ولا يجب القيام بها الا اذا كانت الوسيلة الوحيدة لتحقيق الهدف المشروع او اذا كان هناك عدة وسائل تكون هي الاقل انتهاكا لحق من حقوق الانسان. ويقع عبء اثبات عنصر الضرورة دائما على الدولة.

4. التلاؤم: اي اجراء يجيزه القانون يجب ان يكون متلائما مع الهدف المشروع الذي تم تحديده.

5. التناسب: ان مراقبة الاتصالات يجب النظر اليها كفعل ينتهك حقا اساسيا ويقوض المجتمع الديمقراطي. لذا على القرارات المرتبطة بالمراقبة ان تتعامل مع حساسية المعلومات المنوي الوصول اليها ومدى خطورة انتهاك حقوق الانسان. لذا على الدول ان تتشارك مع السلطات القضائية الصالحة الامور التالية، قبل اجراء التعقب لتنفيذ القانون او حماية للامن القومي او لجمع معلومات استخباراتية:

- هناك احتمال كبير لحصول جريمة خطيرة او تهديد معين على هدف مشروع
- هناك احتمال كبير ان اثبات هذه الجريمة او هذا التهديد سيتم الحصول عليه من جراء الوصول الى المعلومات الشخصية المطلوب تعقبها.
- قد تم اللجوء الى تقنيات اخرى اقل اجتياحا او ليس هناك امكانية للجوء الى تقنيات اقل اجتياحا
- سيتم الاكتفاء بالمعلومة المتعلقة بالجريمة المراد كشفها او التهديد المتوقع.
- كل معلومة اضافية يتم الوصول اليها لا يمكن الاحتفاظ بها وانما يتم اتلافها او اعادتها

- المعلومات يتم الوصول اليها فقط من الجهات المعنية ويتم استخدامها فقط لهدف ومدة الاذن الممنوح للسلطة المعنية.
- على ان لا تقوض افعال المراقبة المطلوبة والتقنيات المقترحة جوهر الحق بالخصوصية او الحريات الاساسية.

6. سلطة قضائية صالحة: قرارات المراقبة يجب ات تصدر عن سلطة قضائية صالحة محايدة ومستقلة. يجب ان تكون هذه السلطة:

- منفصلة ومستقلة عن السلطات التي تجري مراقبة الاتصالات
- مطلعة وصالحة لاتخاذ قرار حول مشروعية مراقبة الاتصالات والتكنولوجيا المستخدمة وحقوق الانسان.
- لديها الموارد الملائمة لممارسة المهام الموكلة اليها

7. الاجراءات القانونية: يجب على الدول ان تحترم وتضمن حق الافراد في ان تكون الاجراءات القانونية واضحة في القوانين ومتوافرة للعامة. فلكل فرد الحق في جلسة استماع علنية عادلة ضمن فترة زمنية مقبولة امام هيئة قضائية صالحة ومحايدة ومحددة في القانون الا في حالات الطوارئ حيث يثبت خطر داهم على الحياة البشرية. في هذه الحالة يجب اخذ اذن ولو بمفعول رجعي في مهلة زمنية معقولة.ولا يمكن اعتبار مجرد خطر ضياع او تدمير الدليل كاف لتعليل الاذن بمفعول رجعي.

8. ابلاغ المستخدم: يجب ابلاغ من يتم تعقب اتصالاتهم بقرار التعقب ليتمكنوا من الطعن في القرار او من تزويد السلطات بالمعلومات المطلوبة.ولا يمكن التأخر بالتبليغ الا في الظروف التالية:

- اذا كان من شأن التبليغ ان يعرض نجاح العملية للخطر او اذا كان هناك خطرا مؤكدا وداهما على الحياة البشرية.
- الاذن بتأخير التبليغ صادر من السلطة القضائية الصالحة

• يتم تبليغ المستخدم المعني عند زوال الخطر كما حددت السلطة القضائية الصالحة.

9. الشفافية: على الدول ان تكون شفافة حول استخدام ونطاق قوانين وممارسات مراقبة الاتصالات، وعليها ان تنشر العدد المحدد للمعلومات المجمعة بناء على الطلبات المقبولة والمرفوضة مع تفاصيل تتعلق بالهدف وبعدد الافراد المستهدفين في كل حالة.

10. جهاز عام للمراجعة: على الدول ان تؤسس آليات مراجعة مستقلة لضمان الشفافية والمحاسبة في ما يتعلق بمراقبة الاتصالات. على هذا الجهاز ان تكون لديه الصلاحية للوصول الى كل المعلومات ذات الصلة بما فيها المعلومات المصنفة سرية، لكي يتمكن من التأكد من مشروعية الهدف ومدى تطبيق موجبات الشفافية والنشر ومدى الملاءمة مع المبادئ العامة.

11. نزاهة الاتصالات والانظمة: من اجل ضمان نزاهة، امن وخصوصية انظمة الاتصالات لا يجب على الدول ان تلزم مزودي الخدمات او شركات البرمجيات ان تبني قدرات مراقبة وتعقب في انظمتها او ان تجمع او تحتفظ بمعلومات تدخل ضمن اهداف مراقبة الاتصالات للدولة، اذ لا يمكن ان يطلب من مزودي الخدمات حفظ البيانات. والمستخدمون لديهم الحق بالتعبير عن نفسهم بهوية مغفلة ولا يجب على الدول ان تلزمهم بالتعريف عن هوياتهم.

12. ضمانات التعاون الدولي: استجابة للتغيرات في تقنيات الاتصال وتداول المعلومات يمكن للدول ان تسعى الى الى طلب المساعدة من دول اخرى او من مزودي خدمات اجانب. على ان يكون المبدأ التجريم الثنائي اذ لا يمكن للدول ان تلجأ الى الطلبات الخارجية لمعلومات محمية للتحايل على قوانينها الداخلية التي تمنع الرقابة على الاتصالات. على ان اجراءات المساعدة القانونية المتبادلة بين الدول يجب ان يتم توثيقها بوضوح واتاحتها علنية ويجب ان تضمن الاجراءات القانونية العادلة.

13. ضمانات لمواجهة الوصول غير المشروع: على الدول ان تنص تشريعات تجرم مراقبة الاتصالات غير المشروعة. على ان تكون هذه القوانين تتضمن عقوبات مدنية وجزائية، فضلا عن حماية الكاشفين. وعلى ان يتم اتلاف كل المعلومات التي تم جمعها بطريقة غير مشروعة.

وبالرغم من عدم وجود احكام قضائية كثيرة في لبنان الا انه تجدر الاشارة الى ان القضاء اللبناني حقق خطوات جريئة لناحية اعتماد المعايير الدولية لاسيما المواثيق والمعاهدات الدولية وفق روحية مقدمة الدستور اللبناني. ويمكن الاشارة هنا الى قرار صادر عام ٢٠١٢ عن قاضي الامور المستعجلة في بيروت جاد معلوف اعتبر فيه انه طالما هو متح وغير متعذر على الخصوم اثبات الواقعة المطلوبة بواسطة الاقرار او شهادة الشهود او خبرة الخبراء او اية وسيلة اثبات قانونية اخرى فليس ما يوجب الزام دوائر حكومية بكشف معلومات ذات طابع شخصي متوافرة لديها احتراما لحق هؤلاء الاشخاص بحماية خصوصيتهم. وفي حيثيات القرار الصادر في ١٦ آب ٢٠١٢ رفض القاضي معلوف طلبا قدمه احدهم يطلب فيه الترخيص له بالحصول على بيانات الامن العام المتعلقة بحركة دخول البلاد والخروج منها لاثبات واقعة ترك المأجور وبالتالي سقوط حقهم بالتمديد كونهم من المستأجرين القدامى. واعتبر القاضي ان الكشف عن هذه المعطيات يتضمن الكثير من المعلومات الشخصية مما يفرض عليه الموازنة بين حق المتقاضي بالحصول على الاثبات المتوفر في سجل الامن العام وحق الخصوم في الحفاظ على بياناتهم عملا بالخصوصية. واعتبر ايضا ان هذه البيانات لدى الامن العام محفوظة لضرورات المصلحة العامة الا انها تبقى خاضعة للحماية كونها معلومات خاصة. وربط المس بهذا الحق بالمادة ١٢ من الاعلان العالمي لحقوق الانسان والمادة ١٧ من العهد الدولي الخاص للحقوق المدنية والسياسية. كما اضاف ان حماية هذا الحق باتت اكبر اليوم في ظل التطورات الاجتماعية الحاصلة والمتمثلة بالتقنيات التي تمكن من اختراق مختلف جوانب الحياة الخاصة للافراد، مستشهدا باجتهادات المحكمة الاوروبية لحقوق الانسان. واعتبر القاضي معلوف ان التضحية بخصوصية المستأجر هنا تكون غير ضرورية لاحتمال ان يتمكن المؤجر من اثبات الوقائع بوسيلة

اخرى لا تتعدى على الحرية الشخصية للغير من بينها اقرار المستأجر او شهادة الجيران او فواتير الكهرباء وغيرها.

المبحث الثالث: الخصوصية وحق المواطنين بالاطلاع

ان الحق في الخصوصية هو اساس الحقوق والحريات الاخرى، بما في ذلك حرية التعبير وحرية التجمع وحرية المعتقد. وتلعب القدرة على التواصل دون الكشف عن الهوية الحقيقية مثلا دورا مهما في حماية التعبير الحر وتعزيز المحاسبة لاسيما في الدول القمعية، وتشجع الناس اكثر للتعبير عن رأيهم في قضايا تهم المصلحة العامة اذا شعروا انهم بمنأى عن التوقيف والانتقام. فحرية التعبير هي اساس الديمقراطية ولا يمكن لمجتمع ان يسائل حكامه الا عبر ممارسة هذا الحق الذي لا يمكن تقييده الا عندما يمس حماية حقوق الاخرين وحرياتهم.

وهنا يمكن للخصوصية ان تتعارض مع الحق بالتعبير ولا بد من ايجاد توازن بين الحقين. ايجاد هذا التوازن ليس سهلا اذ هناك خط رفيع بين التعبير الحر والخصوصية، ويبقى للمحاكم ان تحدد كيفية ادارة العلاقة بين الحقين وتأتي المصلحة العامة في صلب محرك الميزان.

المطلب الاول: الحدود بين حرية التعبير والخصوصية

تتصل حرية التعبير بالخصوصية اتصاقا وثيقا اذ يعتبر الحقان معززان ومكملان لبعضهما، لاسيما في العصر الرقمي. الحقان هما اساسيان لمجتمعات ديمقراطية ومفتوحة ويجب حمايتهما لتعزيز المحاسبة والحوكمة الرشيدة بوجه الدول والشركات الكبرى في ايامنا. في وقت تعتبر حرية التعبير اساسا للتعبير عن التنوع الثقافي والفكري والخلق والابداع، فان الخصوصية ضرورية لضمان استقلالية الفرد وتطوير ذاتهم وتخويلهم بناء علاقات مع الآخرين. كما ان الخصوصية شرط اساسي للممارسة الحرة للحق بالتعبير خاصة على الانترنت. فالافراد يشعرون بأمان اكبر في التعبير عن وجهات نظر جدلية او بمشاركة معلومات قد تكون حساسة فيما لو كانت هويتهم مغفلة او ان خصوصيتهم وامن اتصالاتهم مصانة. بدون الخصوصية

يفتقد الافراد الى مساحات يتمكنون فيها من التفكير والتحدث والتعبير عن رأيهم بدون تدخل. وان احترام سرية الاتصالات مثلا هو امر ضروري لثقة كل من يريد كشف فساد ومطلب رئيسي لممارسة الحق بالتعبير في امور قد تعتبر حساسة في سياق ما.

وقد يصطدم حق احدهم بالتعبير مع حق آخر بالخصوصية. ففي بعض الحالات يمكن لاحدهم ان يتذرع بالخصوصية دون اي مبرر ليمنع نشر معلومات بهدف الحد من نشر قضايا تتعلق بالمصلحة العامة وللتهرب من المضايقات او لتحوير حقائق معينة. كما ان نشر معلومات خاصة دون مبرر يمكن ان تنتهك حق الخصوصية لاسيما بالنسبة للاشخاص الاكثر حساسية. اذا يمكن لهذين الحقين ان يتداخلا ويعززا بعضهما الآخر كما يمكن ان يتنازعا وذلك على الانترنت وخارجه.

واذ يبقى ان النشر والوصول الى المعلومات اساسيان لتعزيز المحاسبة ولتحقيق مجتمعات خالية من الفساد وتعزيز حق الاطلاع. كما ان الانترنت شكل موردا كبيرا حيث عززت تكنولوجيا المعلومات حرية التعبير والوصول الى المعلومات ولكن طرحت في نفس الوقت تحديات جمة تتعلق بحماية خصوصية الافراد وحماية بياناتهم الشخصية.

ان الاطار القانوني لحرية التعبير يجد جذوره في المادة ١٩ من الاعلان العالمي لحقوق الانسان التي تنص على ان:

لكل فرد الحق في حرية التعبير والرأي، ما يعني الحق في عدم القلق بسبب آرائه وبان ينشر من دون اعتبار للحدود الجغرافية وباية وسيلة للتعبير عن آراءه ومعلوماته.

وعرفته ايضا المادة ١٩ من العهد الدولي الخاص للحقوق المدنية والسياسية على اساس ان:

١. لكل إنسان حق في اعتناق آراء دون مضايقة.

٢. لكل إنسان حق في حرية التعبير. ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع أو في قالب فني أو بأية وسيلة أخرى يختارها.

٣. تستتبع ممارسة الحقوق المنصوص عليها في الفقرة ٢ من هذه المادةواجبات ومسؤوليات خاصة. وعلى ذلك يجوز إخضاعها لبعض القيود ولكن شريطة أن تكون محددة بنص القانون وأن تكون ضرورية: أ- لاحترام حقوق الآخرين أو سمعتهم، ب- لحماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة.

وقد وضعت منظمة المادة ١٩ الدولية Article 19 وهي منظمة دولية مرجعية تعنى بتعزيز حرية الرأي والتعبير حول العالم، مبادئ عامة حول حماية حرية التعبير والخصوصية [37] ، عملت عليها عام ٢٠١٦ بطريقة تشاركية مع منظمات معروفة حول العالم في مجال حرية التعبير والخصوصية وذلك انطلاقا من القانون الدولي لحقوق الانسان ومبادئ الامم المتحدة وغيرها من المراجع الدولية المعنية.

وفي خلاصة هذه المبادئ ان على الدول ان تضمن الحق في حرية التعبير، وحق تداول المعلومات والحق في الخصوصية في دساتيرها المحلية او ما يوازيها بما يتلاءم مع قانون حقوق الانسان الدولي. فيكون لكل فرد الحق في التعبير دون تضييق والحق في تداول المعلومات وضمنها حق النقد والتعليق على الآخرين والحق في الخصوصية بما فيها احترام الحياة الخاصة والمنزل والاتصالات والحق بحماية القانون في حال تم التعرض لهذه الحقوق. هذا فضلا عن الحق في حماية البيانات الشخصية المنبثقة والمتعلقة بالحق بالخصوصية.

اما بالنسبة للقيود على حرية التعبير والحق بالخصوصية فيجب ان تكون مبررة اذا سمحت القوانين لاهداف مشروعة وكانت ضرورية ومتناسبة مع الهدف المشروع على ان لا يكون هناك تقييد للحق بابداء الرأي.

---

[37] http://article19.shorthand.com

كما على الدول ان تضمن حماية هذه الحقوق في قوانينها لاسيما من قبل هيئات قضائية مستقلة. كما ان القوانين المتعلقة بالخصوصية يمكن ان تحد من حرية التعبير فقط اذا كانت تطبق بشكل ضيق لحماية الافراد من التعرض لحياتهم الخاصة اة حياة عائلتهم او منزلهم او اتصالاتهم. ولا يمكن للقوانين بذريعة حماية الخصوصية ان تمنع التعرض عن الاشخاص العامين الذين يكون نقدهم واجب لاتصاله بالمصلحة العامة.

ويفترض تداخل حقي التعبير والخصوصية وتكاملهما ان تضمن الدول حق الافراد بان يمارسوا حقهم بالتعبير دون الافصاح عن هوياتهم وان يصلوا الى المعلومات ايضا بطريقة مغفلة وان يكون لهم حق استخدام ادوات الحماية الرقمية وضمنها تقنيات التشفير. كما لا يجب على الدول ان تلزم مزودي الخدمات بالافصاح عن داتا الافراد الا امام القضاء وفق معايير المشروعية والهدف المشروع، الضرورة والتناسب وفق قانون حقوق الانسان الدولي. كما يتضمن حق حرية التعبير الحق بحماية المصادر لاسيما بالنسبة للصحافيين الذين يحق لهم حماية مصادرهم ولا يمكن للدول ان تلزمهم بالافصاح عنها.

اما عند تعارض حقي التعبير والخصوصية لاسيما في قضايا النشر، فيجب ان يراعي نشر المعلومات الخاصة المعايير التالية حسب كل حالة:

- الى اي مدى يساهم المنشور المشكو منه في نقاش يهم المصلحة العامة. والمقصود بالمصلحة العامة الامور التي يكون للرأي العام مصلحة او اهتمام بان يكون مطلعا عليها. هذا يشمل معلومات حول امور يمكن ان تؤثر على اداء الدولة، الاشخاص العامين، الساسة، الصحة العامة، الامان، تطبيق القانون وادارة العدالة، حماية حقوق الانسان، المستهلك، المصالح الاجتماعية، البيئة، القضايا الاقتصادية، ممارسة السلطة، الثقافة والفنون او اية قضايا اخرى تؤثر على المصالح العامة وتؤدي الى نتائج محسوبة.
- درجة شهرة او مدى حساسية الشخص المعني

- موضوع التغطية ومدى توافر الطبيعة الخاصة للمعلومة
- السلوك السابق للشخص المعني
- مضمون، شكل ونتائج المنشور، وضمنه النبرة المستخدمة الساخرة او التي تحتوي على مزاح، والى اي مدى مسّ الضرر المشكو منه عبر مشاركة المعلومات الخاصة بنزاهة الشخص المعني.
- الطريقة التي تم فيها الحصول على المعلومة
- نية الناشر وتحديدا ما اذا توافرت سوء النية
- الى اي مدى يعتبر الشخص الذي تم التعرض لخصوصيته هو شخصية عامة

وفي حال كانت المعلومات المنشورة عبارة عن فيديو او منشورات ينظر الى مدى توافر رضى الفرد المعني بان يتم تصويره او تسجيل حديثه.ولا يمكن السماح بنشر معلومات تم الحصول عليها عبر تقنيات الكاميرات الخفية او غيرها الا اذا كانت المصلحة العامة متوافرة بقوة ولم يكن بالامكان الحصول على المعلومة بطريقة مختلفة.

ان المعيار الاساسي يبقى ان فتح نقاش حول قضايا المصلحة العامة هو في صلب الحياة الديمقراطية. وان الاشخاص العامين لاسيما رؤساء الدول والممثلين المنتخبين والافراد الذين يلعبون دورا في الحياة العامة ويمارسون وظيفة عامة او معنيين في الشأن العام، يجعلون انفسهم اكثر عرضة للمساءلة وحتى للمضايقة من الصحافيين ومن الجمهور. لذا يجب ان يكون لديهم توقعا اقل من الافراد العاديين بالنسبة لخصوصيتهم. اذ ان المصلحة العامة يمكن ان تمتد الى الحياة الخاصة التي يمكن ان تكون مرتبطة او تؤثر على دورهم في الشأن العام ولكن لا تتضمن الامور الخاصة المحض التي لا تكون مهمة بالنسبة للرأي العام الا لكونها مثيرة.

المطلب الثاني: موقف الاجتهاد اللبناني والمقارن

نظرا لتداخل الحق بالخصوصية مع حق المواطنين بالاطلاع، تحتل الاجتهادات القضائية اهمية بارزة هنا لاحقاق التوازن بين الحقين اذ يجب النظر الى كل قضية على حدى وفقا لمبادئ تم ترسيخها في الاجتهاد الدولي لتقييم غلبة اي من الحقين على الآخر لاسيما بالنظر الى صفة الشخصية العامة التي تشكو من انتهاك خصوصيتها. وفعلا قد قال رولان دوماس [38] في كتابه عن الحق بالاعلام انه "ما ان يطالب فرد بمنح المواطنين ثقتهم له والادلاء باصواتهم لصالحه، يجد هذا الفرد نفسه امام حتمية التنازل عن المناعة التي كانت تحمي حياته الخاصة لصالح الكشف عن معلومات اوضح واكثر وفرة حول كل ما يبرر او يدحض لديه هذه الثقة الممنوحة له. وذلك واجب يحتم على الشخصية العامة توفير الشفافية، لاسيما في ذلك الجزء من الحياة الخاصة الذي غالبا ما يتم الابقاء على سريته". من هنا سنستعرض المبادئ التي رسخها الاجتهاد الدولي في قضايا مرجعية وموقف الاجتهاد اللبناني من هذه المبادئ.

أولا: المبادئ التي رسخها الاجتهاد الدولي

من الثابت في القانون الدولي واجتهادات المحاكم الدولية انه في حال نشوء نزاع بين الحق في التعبير والخصوصية ينظر الى المصلحة العامة كمرجعية اساسية من اجل تقرير اي حق يجب مفاضلته. ولعل اشهر القضايا التي وضعت اسسا واضحة لهذه المفاضلة وللمصلحة العامة نجدها في قضيتي فون هانوفر ضد المانيا امام محكمة حقوق الانسان الاوروبية. [39] وقد اصدرت هذه المحكمة قرارين الاول في ٢٠٠٤ والثاني في ٢٠١٢ في قضيتي فون هانوفر ضد المانيا وفون هانوفر ضد المانيا (رقم ٢) وضعت خلالهما قواعد واضحة تتعلق باحترام الحياة الخاصة.

[38] Rolland Dumas, Le Droit de l’Information, Coll. “Themis”, PUF, 1981, p. 550

[39] ٢٤ حزيران، طلب رقم ٥٩٣٢٠/٠٠ و٧ شباط ٢٠١٢، طلب رقم ٤٠٦٦٠/٠٨ ورقم ٦٠٦٤١/٠٨

وتتعلق القضية الاولى بنشر صحف المانية لعدد من صور كارولين اميرة موناكو وهي تمتطي الخيل واثناء عطلة التزلج واثناء تعثرها على شاطئ خاص. وقد أيدت المحاكم الالمانية نشر هذه الصور (باستثناء بعض الصور في اماكن يفهم منها ان الاميرة ارادت احترام حياتها الخاصة وبعض صورها مع اطفالها.)، على اعتبار ان الاميرة شخصية عامة في المجتمع المعاصر ولا يحق لها التمتع بحماية حياتها الخاصة الا في حال كانت متوارية عن انظار الجمهور في مكان منعزل.

وقد حكمت المحكمة الاوروبية بالتالي:

في المسائل التي تتعلق بايجاد توازن بين حرية التعبير وحماية الحياة الخاصة فان المحكمة تتجه دائما الى النظر عما اذا كان نشر الصور او المقالات في الصحف من شأنه ان يساهم في نقاش ذات مصلحة عامة.

واكدت المحكمة على ان:

تعتبر المحكمة انه من الاجدى التمييز بين تغطية صحافية مرتبطة بوقائع، ولو كانت موضع جدل، من شأنها ان تساهم في النقاش في مجتمع ديمقراطي، يتعلق بشخصيات سياسية في معرض قيامهم بوظائفهم العامة مثلا، وبين تغطية صحافية حول تفاصيل الحياة الخاصة لشخصية، مثل الحالة في هذه القضية، لا تقوم بوظائف عامة.

فتكون بذلك المحكمة الاوروبية قد ربطت معيار احترام الحياة الخاصة بمدى ممارسة الشخصية العامة لوظائف عامة. وفي حالة الاميرة كارولين فان اهتمام الصحافة والجمهور مستمد فقط من كونها من العائلة المالكة وليس بمعرض قيامها بوظائف عامة.

اما في القضية الثانية كان الامر يتعلق بصور منشورة تتعلق بمرض الامير رينييه، حاكم موناكو وبكيفية تعاطي عائلته معه اثناء مرضه. في هذه القضية استخلصت المحكمة الاوروبية مجموعة معايير تحدد التوازن بين حرية التعبير وحماية الحياة الخاصة وهي:

- مدى المساهمة في نقاش يهم المصلحة العامة

- درجة شهرة الشخصية المعنية والغرض من التغطية الصحافية
- السلوك السابق للشخصية المعنية
- المحتوى، الشكل وتداعيات المنشور
- ظروف اخذ الصورة

في هذه الحالة وسعت المحكمة من حرية النشر عندما تساهم في نقاش ذات مصلحة عامة. فبعكس القضية الاولى حيث لا تساهم صورة الاميرة كارولين المتعرّية على الشاطئ مثلا في اي نقاش يتعلق بالمصلحة العامة، تأتي خلاصة المحكمة في القضية الثانية لتؤكد ان التقارير والصور حول مرض الامير رينييه وهو حاكم امارة موناكو في ذلك الوقت، وسلوك افراد عائلته اثناء مرضه، يتعلق دون شك بمسألة مصلحة عامة.

ثانيا: مبدا سمو المصلحة العامة في الاجتهاد اللبناني:

في قضية طلب ادارة الجامعة الاميركية في بيروت منع جريدة الاخبار من نشر اي مستندات او مراسلات الكترونية خاصة في القضية المعروفة بـ " AUBليكس"، أصدر قاضي الامور المستعجلة في بيروت نديم زوين قرارا في ٨ كانون الاول ٢٠١٤ رسخ من خلاله مبدأ المصلحة العامة اذ اعتبر ان هكذا نشر جائز "في حال توافر ظروف استثنائية تفرض تفهم نشر مراسلة خاصة، كان يكون مضمون المراسلة يمس سلامة الدولة او امنها او متى كان النشر ضروريا ومهما للمصلحة العامة ذات الشأن الى حد يسمح بالتضحية بالاعتبار الشخصي."

ويجدر ذكر حكم آخر صادر عن قاضي الامور المستعجلة في بيروت بتاريخ ١٨-٠١-٢٠١٤، القاضي جاد معلوف في قضية مستدعية ضد كل من شركة scoop Liban SAL وشركة تلفزيون المستقبل ش. م. ل. تطلب منع عرض حلقة تظهر فيها على تلفزيون المستقبل. رسخ القاضي معلوف مبدأ ان حرية الاعلام مصانة ولكن حرمة الحياة الخاصة واجبة الحماية ايضا ما يوجب الموازنة بين هاتين الحريتين. استند القاضي الى مقدمة الدستور اللبناني التي تلزم لبنان بالمواثيق الدولية وبالتالي الى المواد القانونية في

العهد الدولي الخاص لاسيما المادة ١٩ التي تضمن حرية التعبير وفسر بناء عليه دور الاعلام والصحافة الاساسي في الحياة العامة في نظام ديمقراطي يقوم على تبادل الافكار ونقاش القضايا العامة وتزويد المواطنين بمعطيات لممارسة الرقابة على السلطات. وعاد القاضي وشرح ان حق الجمهور في المعرفة التي تستتبع حرية التعبير والصحافة قد يتم "تبديتها" احيانا على حقوق اخرى مثل الحق في الصورة الشخصية او المحافظة على السمعة او حماية حرمة الحياة الخاصة ولكن لا بد من اجراء موازنة بين الحقوق المتعارضة لتقرير توفير الحماية لاحدها على حساب الاخر. واكد القاضي معلوف ايضا على حق كل شخص بالمحافظة على صورته وسمعته وحياته الشخصية وفق الماد ١٧ من العهد الدولي الخاص والمادة ١٢ من الاعلان العالمي لحقوق الانسان. بالتالي فان حماية الحياة الشخصية توازي حماية حرية الاعلام والتعبير والحق بالمعرفة. وورد في الحكم التالي:

"وحيث في الحالات التي يتواجه فيها كل من حرية التعبير والصحافة وحق الجمهور بالمعرفة من جهة والحقوق الشخصية بحماية الصورة الشخصية والسمعة والحياة الشخصية من جهة أخرى لا بد من التحقق من الهدف الذي يتم السعي إليه وتحديد ما إذا كان يخدم فعلا مصلحة عامة من الواجب اطلاع الجمهور عليها ويوفر المعرفة المطلوبة للجمهور أم انه يشكل تعرضاً غير مبرر لحرمة الحياة الشخصية وصورة الشخص الواجبة الحماية وفقًا للمواثيق عينها التي تحمي حرية التعبير،

وحيث يقتضي إذا عند إجراء الموازاة المذكورة التطرق إلى المسائل التالية، دون ضرورة توافرها بمجملها في كل حالة:

1. هوية الشخص الذي يتم التعرض لحياته الشخصية وتحديد ما إذا كان من الأشخاص المعروفين أو العامين أو الذين يتولون وظيفة عامة أو يتعاطون بعمل يهم العامة،
2. المسألة أو الموضوع الذي يتم التطرق إليه وتحديد ما إذا كانت المسالة هي مسألة خاصة أم مسألة عامة من مصلحة الجمهور معرفتها أو من حقه معرفتها أو أن المصلحة العامة تقضي

بفضحها، كالمسائل المتعلقة بالجرائم أو بالوظيفة العامة أو الفساد مثلاً،

3. التحقق مما إذا كان للشخص المعني توقع معقول بالخصوصية في الحالة المعروضة أو بالنسبة للمسألة التي يتم التطرق إليها أو في المكان الذي يتم التعرض له،

4. التحقق مما إذا كان تم نشر معطيات في السابق بشأن الموضوع عينه ما ينفي بالتالي بعد النشر السابق التوقع المعقول بالخصوصية،

5. التحقق من إمكانية الوصول إلى الغاية المرجوة أو تزويد الجمهور بالمعطيات والمعلومات المطلوبة بطريقة لا تتعرض للحياة الشخصية أو تشكل تعرضاً اقل حدة،

6. تحديد ما إذا كان الشخص وافق صراحة أو ضمناً على النشر.

وحيث من العودة إلى المعطيات المتوفرة في القضية الراهنة يتبين أن المستدعية لا تدخل في عداد الشخصيات العامة أو المعروفة، كما وان المسألة التي يتم عرضها لا تشكل بحد ذاتها مسألة عامة من مصلحة الجمهور معرفتها بل تتمثل بخلاف ذي طابع قانوني مدني خاص قائم بين مؤجر ومستأجر بشأن تنفيذ عقد الإيجار، وإن كان يشكل مثالاً على بعض العلاقات بين المؤجرين والمستأجرين، كما وان إعطاء المعلومات أو التلميحات حول هوية المستدعية ليس من شأنها إضافة أية معلومات يستفيد منها الجمهور ولم يثبت أنها تحقق أية غاية تستوجب الحماية، فضلاً عن أن التصوير تم في مكان خاص للمستدعية التوقع المعقول بالخصوصية فيه.

وحيث يضاف إلى ما تقدم أن المستدعية كررت مراراً رفضها التصوير ورفضها الظهور على الهواء عند الاتصال بها، ولا يمكن اعتبار أن ما نطقت به على الهواء موافقة ضمنية، أولاً في ضوء رفضها الصريح الصادر سابقاً والمكرر لاحقاً وثانياً كون ما نطقت به بقي فقط ضمن ردة الفعل على بعض الأسئلة الموجهة إليها بصورة معينة من مقدم البرامج. وحيث أن ما تقدم وإن كان يبرر تدخل المحكمة لحماية حرمة الحياة الشخصية وصورة المستدعية إلا انه لا يبرر المنع المطلق ذلك أننا أمام حقين جوهريين مستوجبي

الحماية وإنما تصادف أنهما تعارضا في الحالة الراهنة، فيكون تدخل المحكمة لإعادة التوازن الذي اختل بفعل تضارب الحقين وليس لتعديل التوازن لتبديه حق على الآخر بصورة مطلقة، بمعنى آخر، لا يمكن تبرير إصدار المنع المطلق الشامل من النشر إلا متى كان هذا المنع هو الحل الوحيد لرفع التعرض."

وبناء على ذلك حكم القاضي برد طلب منع الحلقة بكاملها والزام الجهة المدعى عليها بعدم عرض الحلقة الا بعد تعديل صوت المستدعية في كل مرة يظهر في الحلقة وتمويه مكان عملها الذي تم تصويرها فيه وتمويه كل ما يظهر الحياة الخاصة للمستدعية.

الفصل الثاني: حماية البيانات الشخصية بين القانون والممارسة والتجارب المقارنة

يرتبط موضوع حماية البيانات الشخصية ارتباطا وثيقا بالحق بالخصوصية. لا بل ان توفير الحماية لمعالجة البيانات الشخصية هو اداة لحماية حق المواطنين بالخصوصية. سنستعرض في هذا الفصل ثلاثة مباحث نعرض من خلالها آليات حماية البيانات الشخصية في القانون المقارن لاسيما في ضوء الاطر الدولية وخاصة اللائحة العامة لحماية البيانات الشخصية التي وضعها الاتحاد الاوروبي ودخلت حيز التنفيذ في العام ٢٠١٨ وما ترتب عن هذه الاطر الدولية من حقوق للافراد وواجبات للدول والشركات الخاصة على حد سواء وكيفية اجراء الرقابة والاشراف على ضمان حماية البيانات الشخصية للافراد. وفي المبحث الثاني سنستعرض القوانين اللبنانية التي تتضمن اطرا لحماية البيانات الشخصية لاسيما احدث قانونين وهما الوصول الى المعلومات وقانون المعاملات الالكترونية وحماية البيانات الشخصية ومدى تلاؤمهما مع المعايير الدولية. وفي المبحث الثالث نورد دراستي حالة عن كيفية التعاطي في لبنان مع موضوع البيانات الشخصية من قبل الادارة العامة ومن قبل القضاء.

المبحث الاول: آليات حماية البيانات الشخصية في القانون المقارن

في المجتمعات الحديثة اليوم، من الضروري ايجاد آليات لحماية البيانات الشخصية للافراد ما يؤمن حماية من التعسف والانتهاكات ولوضع اطر قانونية للشركات والحكومات التي تجمع هذه البيانات، كي لا يمعنوا في جمع بيانات شخصية وتحليلها واستخدامها ومشاركتها دون ان يكون للاشخاص المعنيين اي علم بذلك. بات الفرد يعيش اليوم في زمن يجعله يعطي بعضا من بياناته الشخصية اذا كان يريد استعمال اية خدمة او شراء منتج عبر الانترنت او تسجيل عنوانه الالكتروني او حتى عند زيارة الطبيب او دفع الضرائب او الدخول في علاقات خدماتية او تعاقدية وغيرها من الامور اليومية التي يقوم بها اي فرد. ولا يمكن ان يكون لاي فرد ثقة بالشركات او الادارات العامة والحكومات التي تجمع هذه البيانات الا اذا توفرت آليات

واضحة وفعالة وقوانين تؤمن حماية البيانات الشخصية وتقلل من تعقب الشركات والحكومات واستغلالها للبيانات.

وعملية جمع البيانات تزيد باضطراد كلما اتجهنا الى المكننة والرقمنة ان في الادارات العامة او في الشركات الخاصة. باتت اليوم قواعد البيانات منتشرة ومتطورة تتيح التفتيش فيها وتعديلها ومقاطعتها ومشاركتها مع اي جهة في كافة انحاء العالم. هذا التطور في المجتمعات ادى الى طرح العديد من التسؤلات حول ماذا يحصل ببياناتنا؟ من لديه الحق بالوصول اليها؟ هل تم الاحتفاظ بها بدقة؟ هل يتم تخزينها ونشرها دون علمنا؟وهل تترتب لنا حقوقا عليها وم هي الأليات المتاحة لممارسة هذه الحقوق؟

انطلاقا من هذه الاسئلة بدأت معظم الدول الديمقراطية تضع مبادئ قانونية لحماية البيانات الشخصية. وفي دراسة لمنظمة الخصوصية الدولية Privacy International رصدت المنظمة في كانون الثاني ٢٠١٨ اكثر من ١٠٠ دولة قد اقرت قوانين حماية البيانات الشخصيةواكثر من ٤٠ دولة لديها مسودات قانون او مبادرات لاقرار قانون لحماية البيانات الشخصية.

المطلب الاول: الاطر والتجارب الدولية

ان الاطار القانوني الدولي الاول لحماية البيانات الشخصية نجده في المعاهدة رقم ١٠٨ لحماية الافراد فيما يتعلق بمعالجة البيانات الشخصية . هذه المعاهدة صدرت عن مجلس اوروبا في ١٩٨١ في ستراسبورغ [40]، وتعتبر اول أداة ملزمة تحمي الافراد في وجه الخروقات التي قد تترافق مع جمع ومعالجة البيانات الشخصية كما تنظم في الوقت نفسه تدفق البيانات الشخصية عبر الحدود. كما تحظر معالجة البيانات الحساسة المتعلقة بعرق الافراد اورأيهم السياسي او صحتهم او دينهم او ميولهم الجنسي او سجلهم العدي وغيرها، اذا لم تتوفر اطر حماية واضحة. وتتضمن المعاهدة ايضا حق الفرد بان يعرف ما هي

[40] http://web.archive.org/web/20180523195912/https://www.coe.int/en/web/conventions/full-list/_-/conventions/treaty/108

البيانات الشخصية المتعلقة به المخزنة ليتسنى له اذا وجد ضرورة بطلب تصحيحها. وتفوض المعاهدة بعض القيود على تدفق البيانات الشخصية العابر للحدود بين الدول اذا لم تكن القوانين تتضمن درجة حماية معادلة.

هذا فضلا عن إرشادات منظمة التعاون الاقتصادي والتنمية OECD لحماية الخصوصية وتدفق البيانات الشخصية العابرة للحدود المعروفة بإرشادات ١٩٨٠، العام الذي صدرت فيه بصيغتها الاولى لمواجهة المخاوف من الاستخدام المتزايد للبيانات والمخاطر على الاقتصاد العالمي الناتج عن القيود على تدفق المعلومات عبر الحدود. تضمنت هذه الارشادات اهم مبادئ الخصوصية المتوافق عليها دوليا والتي استوحت منها معظم الدول الاعضاء في المنظمة على مستوى تشريعاتها الداخلية. وفي تموز ٢٠١٣ أقر مجلس منظمة التعاون الاقتصادي والتنمية نسخة معدلة لتوصيات حول الارشادات التي تحكم حماية الخصوصية وتدفق البيانات الشخصية العابر للحدود، وذلك في ضوء المتغيرات التكنولوجية، الاسواق وسلوك المستخدمين، وتنامي اهمية الهويات الرقمية.[41]

تطبق هذه الارشادات على البيانات الشخصية ان في القطاع العام او الخاص، التي تشكل تهديدا للخصوصية والحريات الفردية بسبب طريقة معالجتها او بسبب طبيعتها او بسبب السياق الذي تستخدم فيه. وان اي استثناءات لهذه الارشادات بما فيها تلك المتعلقة بالسيادة الوطنية والامن القومي والنظام العام يجب ان تكون "اقل ما يمكن" وان يتم اعلانها للجمهور. ومن المفيد استعراض المبادئ الاساسية التي اعتمدتها هذه الارشادات لاستخدامها على المستوى الوطني.

- مبدأ تقييد الجمع: يجب ان يكون هناك حدود لجمع البيانات الشخصية وعلى كل جمع لهذه البيانات ان يتم بطرق مشروعة وعادلة، وحيث يكون مناسبا، مع علم ورضى الشخص المعني.

---

[41] اطار الخصوصية الذي وضعته منظمة التعاون الاقتصادي والتنمية/ The OECD Privacy Framework، http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

• مبدأ ضمان نوعية البيانات: البيانات الشخصية يجب ان تكون متوافقة مع الاهداف التي سوف يتم استخدامها من اجلها وبحدود ما هو ضروري لهذه الاهداف كما يجب ان تكون دقيقة وكاملة ومحدثة.

• مبدأ تحديد الهدف: يجب ان تكون الاهداف التي يتم الجمع من اجل تحقيقها محددة في وقت تجميع البيانات واي استخدام لها في حدود تحقيق هذه الاهداف مع ضرورة تحديدها في كل مرة قد تتغير فيها هذه الاهداف.

• مبدأ تقييد الاستخدام: لا يجب نشر البيانات الشخصية او استخدامها لغير الاغراض التي حددت من اجلها الا في حالتين: موافقة ورضى الشخص المعني او بقوة القانون.

• مبدأ ضمان امن البيانات: يجب ان تكون البيانات محمية بضمانات امن معقولة بوجه مخاطر فقدانها او خرقها او تلفها او استخدامها او تعديلها او نشرها.

• مبدأ الانفتاح: يجب ان يكون هناك سياسات مفتوحة حول التطورات والممارسات والسياسات المتعلقة بالبيانات الشخصية. اي ان يتمكن الاشخاص المعنيون من الربط بين المعلومات المتعلقة بطبيعة البيانات الشخصية والاهداف الاساسية وراء استخدامها كما هوية ومحل اقامة القيم على هذه البيانات.

• مبدأ اشراك الافراد: يجب ان تتوفر للافراد الحقوق التالية:

- الحصول من القيم على البيانات على تأكيد او نفي وجود اي بيانات شخصية متعلقة به.
- التواصل مع الشخص المعني فيما يتعلق باي بيانات شخصية متعلقة به في مدة معقولة، وبكلفة، اذا اقتضت، غير عالية، وبطريقة معقولة وبشكل يمكن قراءته.
- تعليل اي طلب رفض حول وجود البيانات او عدمها او التواصل بشأنها، على ان يكون للشخص المعني مراجعة الرفض.

- مراجعة البيانات المتعلقة بالشخص المعني بحيث اذا ما قبلت المراجعة يتم محو البيانات او تصحيحها او استكمالها او تعديلها.

• مبدأ المساءلة: يجب ان تتم مساءلة ومحاسبة اي قيم على البيانات وفق المبادئ المشار اليها اعلاه.

ولعله من المهم ذكر كل من اللائحة العامة للاتحاد الاوروبي لحماية البيانات الشخصية والتجربة الفرنسية كاطر يمكن البناء عليها في التجارب المحلية.

ولا: اللائحة العامة للاتحاد الاوروبي لحماية البيانات الشخصية GDPR

يشكل تاريخ ٢٥ أيار ٢٠١٨ تاريخا مفصليا لحماية البيانات الشخصية مع دخول إرشادات الاتحاد الاوروبي لحماية البيانات الشخصية التي وضعت في ٢٦ نيسان ٢٠١٦ حيز التنفيذ. هذه اللائحة [42] كما تصفها رئيسة الهيئة الوطنية للحريات والمعلومات السابقة إزابيل فالك بروتان [43]، تأتي بتغييرات على مستويات ثلاث:

على المستوى الثقافي، اصبح هناك منطق مساءلة مبني على عقوبات مضخمة. سيصبح على كل من يعالج البيانات ان يتحقق من امتثاله في كل وقت وليس فقط اثناء جمع البيانات ورضى الشخص المعني حينها.

على مستوى الادوات، اصبح هناك سجل لمعالجة البيانات، تحليل لأثرها على الحياة الخاصة، مدونات سلوك، شهادات، كلها أدوات تساعد القطاعات والمشغلين على التقيد بالمبادئ العامة.

---

[42] نص ارشادات الاتحاد الاوروبي لحماية البيانات الشخصية GDPR، https://eur-lex.europa.eu/eli/reg/2016/679/oj

[43] Protection des Données Personnelles, Se mettre en conformité d'ici le 25 Mai 2018, Editions Legislatives, Préface

على مستوى الحوكمة، فان المفوضين لحماية البيانات الذين يتم تعيينهم بطريقة ملزمة في بعض الاحيان سيكونون داخل اجهزتهم القيمين الاساسيين على الامتثال وسيقومون بنشر هذه الثقافة الجديدة ويحثون على استخدام الادوات الجديدة.

تنطلق ارشادات الاتحاد الاوروبي من مبدأ حماية البيانات منذ التصميم وبشكل افتراضي. اي ان الشركات والمنظمات والهيئات العامة يجب ان تأخذ الخصوصية بعين الاعتبار منذ تصميم اية تكنولوجيا تقوم بمعالجة بيانات شخصية الى تنفيذها وتشغيله. قبل هذه الارشادات كان عبء تأمين حماية الخصوصية على المستخدم صاحب البيانات عبر تغيير الاعدادات او الانسحاب من خاصية معينة الخ. اما بعد ارشادات الاتحاد الاوروبي اصبح المبدأ معكوسا اي كل من يصمم تكنولوجيا يجب ان تبني فيها معايير الخصوصية لتقدم افتراضا الى المستخدم (per default). وتتضمن ارشادات حماية البيانات الشخصية ٩٩ مادة ويهدف بالاساس الى حماية الحريات والحقوق الاساسية للاشخاص الطبيعيين لاسيما حقهم بحماية بياناتهم الشخصية. هذا بالاضافة الى تسهيل التدفق الحر للبيانات داخل الاتحاد الاوروبي. وسنعول على التعريفات والمبادئ والحقوق والواجبات المترتبة على حماية البيانات استنادا الى العددي من مواد هذه الارشادات.

ثانيا: التجربة الفرنسية

تعتبر التجربة الفرنسية في حماية الخصوصية والبيانات الشخصية من الاهم لاسيما ان هذا الموضوع شكل هاجسا تشريعيا منذ العام ١٩٧٨ مع القانون الفرنسي لحماية البيانات وذلك قبل اي طفرة تكنولوجية. هذا القانون أنشأ هيئة ادارية مستقلة اسمها الهيئة الوطنية للمعلومات والحريات CNIL في العام ١٩٧٨. ان استقلالية هذه الهيئة مضمونة من خلال تشكيلها وتنظيمها. معظم أعضائها (١٢ عضوا) منتخبون من الهيئات (البرلمان، المجلس الاقتصادي الاجتماعي البيئي) ومن القضاء، وبعض الاعضاء

(٥ أعضاء) هم اشخاص عامون معينون من رئيس مجلس النواب ورئيس مجلس الشيوخ والحكومة. اما مهام هذه الهيئة [44] فهي:

- الاعلام والتعليم: تقوم بحملات توعية عبر موقعها او عبر الاعلام ومواقع التواصل الاجتماعي والورش كما تشارك في المؤتمرات بهدف الاعلام والاستعلام.
- حماية حقوق المواطنين: اي مواطن يمكن ان يتواصل مع الهيئة اذا ماواجه تحديات في ممارسة حقوقه على بياناته الشخصية، لاسيما حق الوصول والاعتراض والتصحيح. وبذلك تستقبل شكاوى تتعلق بالسمعة الرقمية مثل طلبات محو بيانات عن الانترنت، وشكاوى تجارية لوقف الدعاية عبر الايميل مثلا وشكاوى تتعلق بالموارد البشرية مثل آليات الرقابة في التعقب عبر الفيديو، وكذلك شكاوى تتعلق بالمصارف والقروض مثل الاعتراض على تسجيل بيانات في ملفات البنك الفرنسي.
- التنظيم وتقديم الاستشارات: تقوم الهيئة باعطاء آراء رسمية للحكومة حول مشاريع قوانين لجهة أثرها على حماية البيانات. كما تقوم بوضع أطر قانونية لتبسيط استكمال الشكليات المطلوبة وغيرها من القرارات التنظيمية.
- مراقبة الامتثال: يشكل المسؤولون عن حماية البيانات شبكة خبراء يساهمون بوضع رزمة الامتثال لتستفيد منها الشركات الكبيرة المتعددة الجنسيات التي يتم فيها تبادل كثيف للبيانات. ولدى الهيئة صلاحية اعطاء الشهادات للمنتجات التي تتعاطى مع حماية البيانات، ما يعطي ثقة اكبر بهذه المنتجات تجاه المستخدمين.

---

[44] https://www.cnil.fr/en/cnils-missions

• الدفع بالابتكار: تأخذ الهيئة بعين الاعتبار العوامل التكنولوجية المستجدة والوجهات الجديدة لاستخدام البيانات وتقوم بتقييم دراسات حالة وتحليلها اذا ما كانت تستخدم ادوات مبتكرة، وذلك عبر مختبرها والعديد من النشاطات الاخرى التي تقوم بها.

• التفتيش وتوقيع العقوبات: هذه الصلاحية تسمح للهيئة بالتأكد من تنفيذ القانون. ويمكن للهيئة توقيع العديد من العقوبات بدءا بالانذار الذي يمكن ان يكون عاما وصولا الى الغرامة المالية، فيما عدا معالجة البيانات من قبل هيئات حكومية، قد تتراوح بيم ١٥٠ و ٣٠٠ الف يورو ويمكن ان تكون عامة. كما يمكن ان تقرر وقف التوقف والكف عن معالجة البيانات بامر منها، او يمكن ان تسحب الموافقة المبدئية التي اعطتها.

المطلب الثاني: تعريف حماية البيانات الشخصية والحقوق المترتبة للافراد

ان حماية البيانات الشخصية ضرورية لممارسة الحق بالخصوصية. في شرحنا في الفصل الاول للاطر القانونية الدولية للخصوصية وجدنا ان الحق بالخصوصية معترف به كحق من حقوق الانسان في الاعلان العالمي لحقوق الانسان لاسيما في المادة ١٢، كما في المادة ١٧ من العهد الدولي الخاص للحقوق المدنية والسياسية. وفي العام ١٩٨٨، اعترفت هيئة حقوق الانسان في الامم المتحدة، وهي الجهة المولجة بمراقبة تطبيق العهد الدولي الخاص بضرورة وجود قوانين لحماية البيانات الشخصية بغية ضمان الحق بالخصوصية المنصوص عنه في المادة ١٧ وفق ما يلي :[45]

"ان جمع ومسك معلومات خاصة على الكومبيوترات وبنوك الداتا واية اجهزة اخرى، ان عبر سلطات عامة او افراد او اجهزة خاصة، يجب ان يكون منظما بقانون...لكل فرد الحق بان يتأكد بشكل واضح ما هي البيانات الشخصية المخزنة في ملفات بيانات تلقائيةولاية غاية. وكل فرد يجب ان يكون قادرا على التأكد

[45] قرار هيئة حقوق الانسان في الامم المتحدة: UN Doc. HRI/GEN/1/Rev.9, General Comment No. 16: Article 17, para 10

اذا ما كانت اية سلطات عامة او افراد او اجهزة خاصة يتحكمون او يمكن ان يتحكموا بملفاتهم. اذا تم جمع هذه الملفات او معالجتها بصورة مخالفة لما تقتضيه القوانين، كل فرد يجب ان يكون له الحق بطلب تصحيحها او الغائها."

كذلك وضعت الهيئة العامة للامم المتحدة في كانون الاول ٢٠١٦ قرارا بالاجماع حول حق الخصوصية في العصر الرقمي [46] شددت من خلاله ان على الدول احترام موجبات حقوق الانسان الدولية فيما يتعلق بحق الخصوصية لاسيما عندما يطلبون كشف بيانات شخصية من اطراف ثالثين بما فيها الشركات الخاصة.

اذا ان الحق بالخصوصية وحماية البيانات الشخصية مربوطان ببعضهما بصورة تكاملية. ومن المهم لمن يتعاملون بالبيانات ان يأخذوا كافة الاجراءات لحماية البيانات الشخصية وبذلك تحاشي انتهاك الحق بالخصوصية. ان حماية البيانات تتعلق بضمان حق اساسي من حقوق الانسان هو الحق بالخصوصية عبر تنظيم معالجة هذه البيانات. ويتوفر ذلك باعطاء حقوق لكل فرد فيما يتعلق ببياناته الشخصية، ووضع انظمة للمحاسبة وموجبات واضحة للذين يتحكمون او يقومون بمعالجة البيانات.

ان حماية البيانات الشخصية هو مظهر اساسي للحق في الخصوصية. وقد تم ادراج حماية الخصوصية كحق بحد ذاته في ميثاق الحقوق الاساسية للاتحاد الاوروبي عام ٢٠١٢. فالى جانب المادة ٧ من الميثاق التي تضمن الحق بالخصوصية، اتت المادة ٨ لتضمن حماية البيانات الشخصية وفق ما يلي:

١- لكل فرد الحق بحماية البيانات الشخصية اليي تتعلق به.

٢- معالجة هذه البيانات يجب ان تتم بطريقة عادلة لاهداف محددة وعلى اساس رضى الشخص المعني او اسس قانونية مشروعة وموضوعة في القانون. لكل فرد الحق في الوصول الى البيانات المجموعة حوله وله الحق بتصحيحها.

٣- وللامتثال بهذه القواعد، يجب ان تخضع لرقابة هيئة مستقلة.

---

[46] قرار الهيئة العامة في الامم المتحدة رقم ١٩٩/٧١

وسنفصل أدناه في ضوء المعايير الدولية تعريف البيانات الشخصية ومفهوم معالجتها والحقوق المترتبة للافراد وعنصر الرضى وموجبات الجهة المعالجة للبيانات والهيئة الشرفة المستقلة.

اولا: تعريف البيانات الشخصية

يمكن الاستناد الى تعريف ارشادات الاتحاد الاوروبي لحماية البيانات الشخصية،وهي اي معلومات متعلقة بشخص طبيعي يمكن التعرف اليه او لا؛ الشخص الطبيعي الذي يمكن التعرف عليه بشكل مباشر او غير مباشر لاسيما عبر الرجوع الى عنصر تعريف مثل الاسم،رقم تعريف، بيانات موقع، اي تعريف رقمي يعود لعامل او اكثر خاص بالهوية الجسدية او النفسية او الجينية او العقلية او الاقتصادية او الثقافية او الاجتماعية لشخص طبيعي. وطبعا ان البيانات الشخصية التي يمكن تجميعها ومعالجتها هي بتطور وازدياد دائم مع التطور التكنولوجي والرقمي. مثلا اليوم عنوان بروتوكول الانترنت IP Address اصبح يعتبر من البيانات الشخصية.

ومن الامثلة على البيانات الشخصية:

- اسم او عائلة
- عنوان المنزل
- عنوان بريد الكتروني
- رقم تعريف بطاقة
- بيانات الموقع مثلا على الهاتف الذكي المحمول
- عنوان بروتوكول الانترنت
- رقم التعريف الخاص بالهاتف
- البيانات المحفوظة لدى المستشفى او الطبيب

هناك نوع اضافي من البيانات الذي يمكن وصفه بالبيانات الحساسة وهي تستوجب حماية اكبر ونادرا ما يتم تعريفها في القوانين ولكن نجدها في لوائح عديدة منتشرة ويمكن اعطاء عدة امثلة:

- الاصل العرقي او الاثني لاي فرد
- الآراء السياسية
- المعتقدات الدينية او الفلسفية
- عضوية في نقابة
- الصحة الجسدية او العقلية
- الميول الجنسية
- البيانات البيومترية
- البيانات المالية
- ارقام الضمان الصحي
- البيانات المتعلقة بالاولاد

ثانيا: معالجة البيانات الشخصية

ايضا بالاستناد الى ارشادات الاتحاد الاوروبي لحماية البيانات الشخصية يمكن تعريف معالجة البيانات باي عملية او مجموعة عمليات تجرى على البيانات الشخصية او على مجموعة بيانات، عبر وسائل آلية او لا، مثل جمع، تسجيل، تنظيم، هيكلة، تخزين، تكييف او تغيير، سحب، معاينة، استخدام، الكشف عن طريق الارسال، النشر او اي وسيلة لجعلها متاحة، مواءمتها او دمجها، منع، محو او تدمير.

ان المسؤول عن معالجة البيانات قد يكون شخصا طبيعيا او معنويا من القطاع العام او الخاص يقوم بمعالجة البيانات ويقوم بذلك بتحديد كيفية المعالجة والهدف منها.

كما ان معالجة البيانات ممكن ان تتخذ شكل المعالجة الآلية عبر استخدام البيانات الشخصية لتقييم بعض المظاهر الشخصية التي تعود لشخص طبيعي لاسيما لتحليل او توقع مظاهر تتعلق باداء الشخص المعني في العمل، وضعه الاقتصادي، الصحي، افضلياته الشخصية، اهتماماته، سلوكه، موقعه وتحركاته.

ليس هناك معايير متفق عليها عالميا لحماية البيانات الشخصية ولكن يمكن استخلاص هذه المبادئ من توصيات الاجهزة الاقليمية والدولية التي ساهمت في وضع اسس متفق عليها دوليا عبر مدونات، ممارسات، قرارات، توصيات وادوات سياسات.

وعليه هناك ضرورة لوجود قانون واضح لحماية البيانات. يجب على الهيئات العامة والخاصة التي تجمع وتستخدم البيانات الشخصية ان تلتزم معالجة البيانات بحسب هذا القانون الذي يجب ان يضمن التالي :[47]

- يجب ان يكون هناك حدود لجمع البيانات الشخصية، ويجب ان يتم الحصول عليها بطرق مشروعة وعادلة، كما يجب القيام بذلك بطريقة شفافة.
- ان الاهداف التي يراد منها استخدام البيانات الشخصية يجب ان تكون محددة في وقت جمعها، ويجب ان تستخدم فقط للاهداف المتفق عليها. يمكن نشر، استخدام وحفظ البيانات الشخصية فقط في حدود الاهداف الاساسية الا في حال موافقة الشخص المعني او بحكم القانون: بناء على ذلك يجب ازالتها عندما لا تعود ضرورية للغرض الاساسي.
- البيانات الشخصية المجمعة والمعالجة، يجب ان تكون كافية، ذات صلة ومقتصرة على ضرورة الاهداف التي من اجلها يتم استخدامها.
- يجب ان تكون البيانات دقيقة وكاملة ويجب اتخاذ التدابير اللازمة لضمان انها محدثة.

---

[47] دليل السياسات حول حماية الخصوصية، منظمة الخصوصية الدولية، ص ١٥
https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

- يجب اتخاذ ضمانات معقولة لحماية البيانات الشخصية من الضياع، الوصول غير المصوح به، التدمير، الاستخدام، التعديل او النشر.
- لا يجب ان يكون هناك تجميع او معالجة سرية للبيانات. يجب على الافراد ان يعلموا بان بياناتهم يتم تجميعها ومعالجتها، وان يعلموا بالاهداف لاستخدامها، ومن يتحكم بها ومن يعالجها.
- يجب ان تتوفر للافراد حقوق تخولهم التحكم ببياناتهم الشخصية واية معالجة لها.
- من يستخدمون بيانات شخصية يجب ان يكونوا عرضة للمساءلة وان يثبتوا امتثالهم مع المبادئ اعلاه، وان يسهلوا ممارسة هذه الحقوق، وان يلتزموا بالقوانين المطبقة التي تتضمن هذه المبادئ.

وفي كل الاحوال تتجه كافة الدول اليوم الى صياغة قوانين خاصة بحماية البيانات الشخصية. هذه القوانين الخاصة يجب ان تشدد على حماية حق اساسي هو الحق بالخصوصية وبحماية البيانات الشخصية ويقتضي بذلك الغاء كافة القوانين او الاحكام التي تتعارض مع هذه الحقوق الاساسية، اذ هناك قوانين عديدة مثل قوانين الاتصالات او المعلوماتية والتكنولوجيا او التجارة او الحكومة الالكترونية او المالية والمصارف او الامان السيبراني وغيرها قد تتداخل مع حق الخصوصية وحماية البيانات الشخصية ويقتضي بذلك كل ما يتعارض مع المبادئ التي ذكرناها فيما يتعلق بحماية البيانات الشخصية.

ثالثا: الحقوق المترتبة للافراد

تترتب على حماية البيانات الشخصية المرتبطة بحماية حق اساسي هو الحق بالخصوصية، سلسلة حقوق يجب ان يعمل اي قانون خاص بحماية البيانات الشخصية على ضمانها وان يتم فرضها امام الهيئة المختصة بحماية البيانات والمحاكم المعنية.

- الحق بالمعلومات: يجب ان يتم اعلام كل فرد عن كيفية معالجة بياناته الشخصية مهما كانت طريقة جمع هذه البيانات. يجب ان يتم اعلامه بهوية من يحصل على البيانات وتفاصيل الاتصال به، الهدف من المعالجة، كيف سيتم تصنيف البيانات والى من ستصل وكيف ستتم حمايتها، والى اي وقت سيم

تخزينها والحقوق التي يتمتع بها صاحب البيانات وحقه بتقديم شكوى الى هيئة حماية البيانات، ما اذا كان اعطاء البيانات اختياري او الزامي وعواقب عدم اعطاء البيانات. كل هذه المعلومات عن معالجة البيانات ضرورية ليقرر الفرد ما اذا كان يريد استخدام جهاز ما او الاستفادة من خدمة ما عبر مشاركة بياناته الشخصية.

- الحق بالوصول: يحق للفرد ان يطلب معلومات حول ما اذا كانت اية شركة او ادارة تحفظ او تعالج بياناته الشخصية ويجب على الجهة المعنية ان تفصح عن ذلك وعن الاهداف التي تحتفظ او تعالج فيها البيانات ومع من تمت مشاركتها والى اي وقت سيتم الاحتفاظ بها وكيفية حمايتها. ويشكل هذا الحق وسيلة مهمة للافراد وللمجتمع المدني ليتحققوا ويراجعوا كيف يتم التعاطي مع البيانات الشخصية. ويأتي ذلك ضمن مبدأ سياسة الانفتاح الواجب اعتمادها في موضوع التعامل مع البيانات الشخصية.
- الحق بالتصحيح، بالمنع وبالمحو او الحق بالنسيان: يحق للفرد المعني ان يصحح او يمنع البيانات المعالجة المتعلقة به لضمان دقة هذه البيانات وكمالها وحدثيتها وانه لا يتم استخدامها وهي بموضع عدم دقة. لذا لكل فرد الحق بطلب تصحيح او تحديث او تعديل البيانات المتعلقة به اذا كانت غير دقيقة، مغلوطة، مضللة او غير كاملة. كما يحق للفرد ان يمنع معالجة هذه البيانات في ظروف معينة لغاية حل المسالة. كما يحق للفرد في حالات معينة مثلا اذا لم تكن عملية المعالجة مستندة الى اساس قانوني ان يطلب محوها. وهنا ينظر الى عنصر المصلحة العامة من الاحتفاظ بالبيانات موضوع طلب المحو. ولعل هذا الحق بالنسيان هو من الحقوق المستجدة التي اخذت شهرة واسعة لاسيما بعد حكم المحكمة الاوروبية في قضية غوغل ضد اسبانيا في العام ٢٠١٤. شكل هذا الحكم سابقة لجهة ترسيخ الحق بالنسيان، حيث حكمت المحكمة ان المواطنين الاوروبيين لديهم حق تجاه شركات البحث التجارية مثل غوغل والتي تجمع بيانات شخصية بهدف الربح، بان تزيل هذه الشركات الروابط للمعلومات الشخصية اذا ما طلب الشخص المعني على ان تكون هذه المعلومات غير ذي صلة حينها. لم تحكم

المحكمة ان الصحف يجب ان تزيل المعلومات بل وجدت المحكمة ان الحق الاساسي بالخصوصية هو اهم من المصالح الاقتصادية والتجارية للشركات وفي بعض الاحيان حتى اهم من المصلحة العامة في الوصول الى المعلومات. وفي حيثيات القضية، كانت المحكمة الاوروبية قد صدقت قرار هيئة حماية البيانات الاسبانية التي تمسكت بالحريات الصحافية وردت طلب ازالة تقرير صحافي حوول قضية افلاس شخصية من الموقع الالكتروني للمؤسسة الاعلامية[48]. وقد نصت المادة ١٧ من اللائحة العامة الاوروبية صراحة على حق صاحب البيانات بالحصول من مراقب البيانات على محو البيانات الشخصية المتعلقة به وعلى الاخير موجب ازالتها دون تأخير. ويرتبط هذا الحق بحق الوصول الى البيانات الذي لن يكون له معنى اذا لم يعط الفرد حق التصرف ببياناته اذا لم يعد راضيا عن معالجتها، او عندما يحصل خطأ في ذلك او عندما يرى انه من غير الضروري تخزينها. في هذه الاحوال يحق له طلب محوها. ولكن هذا الحق ليس مطلقا اذ سيؤدي بحسب العديد من الانتقادات الى اعادة كتابة التاريخ. لذا وضعت اللائحة العامة الاوروبية حدودا لهذا الحق في المادة ١٧ المذكورة. هذه الحالات التي يحق فيها طلب محو البيانات تتعلق بانتهاء الضرورة من جمعها للهدف التي جمعت من اجله، سحب رضى صاحب البيانات، اعتراض صاحب البيانات على مشروعية جمعها ومعالجتها، اعتراض المعني لمعرفته ان جمع بياناته يتم لاغراض التسويق، انفاذا لحكم قضائي او موجب قانوني. كما ان هناك حالات لم يمكن معها التجاوب مع طلب المحو لاسيما عندما يتداخل حق النسيان مع ممارسة حرية التعبير والمعلومات، او تكون معالجة البيانات امتثالا مع موجب قانوني او لممارسة مهام تتعلق بالمصلحة العامة او ضرورية لاهداف تتعلق بالصحة العامة او لاية ادعاءات اخرى قانونية[49].

---

[48] خلاصة حكم المحكمة الاوروبية في قضية غوغل ضد اسبانيا: https://epic.org/privacy/right-to-be-forgotten/

[49] تفسير الحق في النسيان وفق موقع ارشادات الاتحاد الاوروبي لحماية البيانات الشخصية: https://gdpr.eu/right-to-be-forgotten/?cn-reloaded=1&cn-reloaded=1

- الحق بالاعتراض: يحق للفرد ان يعترض في اي وقت على معالجة بياناته وعلى الجهة التي تقوم بالمعالجة ان تثبت ضرورة استكمال معالجة بيانات الشخص المعني. وفي بعض الحالات يكون حق الاعتراض مطلقا لاسيما في ما يتعلق بمسائل التسويق.

- الحق في نقل البيانات: لكل فرد ان يطلب نقل بياناته بشكل قابل للقراءة الى جهة معينة بموافقته. هذا الحق يأتي لترسيخ السلطة المطلقة لاي فرد على بياناته الشخصية.

- الحقوق المتعلقة بالتصنيف وباتخاذ القرار آليا: ان آلية التصنيف تعتمد اكثر فاكثر لاهداف عديدة تتعلق بالاعلان الهادف والمسوحات الصحية او حتى التوقعات البوليسية. هذا التصنيف يؤدي الى تقييم الافراد حسب تقاطع البيانات الشخصية المجمعة والمعالجة. كذلك الامر بالنسبة لبعض البرمجيات التي تصنف آليا الاشخاص لوضعهم في خانات معينة واتخاذ قرارات بشأنهم. هذه المعالجات يجب ان تخضع ايضا للمبادئ العامة المتعلقة بان تكون المعالجة لهدف مشروع واعلام الافراد المعنيين وحقهم بالتصحيح اذا ما ارتأوا ذلك، كما يجب منع اتخاذ قرارات بشأن افراد استنادا فقط للتجميع والمعالجة الآلية للبيانات.

- الحق بالطعن الفعال: لكل فرد اعتبر ان حقوقه انتهكت بسبب معالجة بياناته الشخصية بطرق مخالفة للقانون ان يلجأ الى طرق طعن فعالة بوجه الجهة التي عالجت البيانات. يجب ان يكون للفرد المعني الحق بتقديم شكوى الى هيئة مشرفة مستقلة. وهذا يستتبع ضرورة وجود هيئة مشرفة مستقلة لديها صلاحية استلام الشكاوى من الافراد المعنيين والتحقيق فيها ومعاقبة المنتهك او احالة القضية الى محكمة مختصة. كما يجب ان يكون للفرد المتضرر الحق بالطعن بقرار الهيئة اذا لم تستجب الى مطالبه. كما يجب اعطاء الحق لمنظمات المجتمع المدني بتقديم شكاوى جماعية بوجه جهة يتضح انها لا تحترم حماية البيانات الشخصية التي تعالجها اذ احيانا يصعب على الافراد ان يكون لديهم المعرفة والموارد للقيام بشكاوى فردية.

- الحق بالتعويض والمسؤولية: يجب ان يتوفر الحق بالتعويض للفرد الذي انتهكت حقوقه بسبب الضرر الذي حدث له ماديا او معنويا. طبعا هناك بعض الاستثناءات التي غالبا ما تتعلق بالسلطات العامة التي تقوم بمعالجة البيانات لاسيما وكالات الامن والاستخبارات. ولكن على هذه الاحوال ان تكون الاستثناءات مذكورة بالتفاصيل لتبيان الظروف التي يمكن لحقوق الافراد المعنيين ان تكون محدودة. وعلى هذه الحالات ان تكون محدودة، ضرورية ونسبية وواضحة للشخص المعني ويستطيع الوصول اليها.

رابعا: الرضى

يشكل الرضى مبدأ اساسيا في حماية البيانات اذ يتيح للشخص المعني ان يتحكم بالبيانات الشخصية المتعلقة به والتي تتم معالجتها. هذا الامر يتعلق بممارسة حقوق اساسية تتعلق بالاستقلالية وتقرير المصير. يجب ان يعطى الرضى بحرية وان يكون محددا وغير غامض ويمكن ان يكون خطيا وبالوسائل الالكترونية. يجب ان يكون صريحا ويتطلب فعلا من الفرد. ويمكن تعريف الرضى بحسب ارشادات الاتحاد الاوروبي لحماية البيانات الشخصية بان "رضى صاحب البيانات يعني اي اشارة تدل على ارادة الشخص المعني، معطاة بحرية ومحددة ومطلعة وغير غامضة، يستخلص من خلالها ان الشخص المعني عنى موافقته عبر تصريح او فعل ايجابي واضح، على معالجة البيانات الشخصية المتعلقة به."

وبالتالي لا يعتد بالقبول اذا كان ضمنيا ويستتبع ذلك ايضا ان يكون لاي فرد الحق بسحب رضاه في اي وقت. وعلى اي جهة تقوم بجمع ومعالجة البيانات ان تبلغ الشخص المعني بامكانية سحب هذا الرضى.

ولا يجب على من يعالج البيانات ان يتذرع بالرضى للتخلف عن باقي الموجبات لاسيما المبادئ الاساسية لحماية البيانات الشخصية وضمنها الشفافية والدقة والهدف المشروع واخذ اقل ما يمكن.

خامسا: موجبات الجهة المعالجة للبيانات

على الجهة التي تعالج البيانات ان تبرهن كيف تمتثل مع موجبات حماية البيانات المختلفة. على هذه الجهات وضمنها الادارات العامة ان يكون لديها القدرة التنظيمية والتقنية لاثبات ان معالجة البيانات لديها يتم وفق القوانين وعليها ان تعتمد من اجل ذلك سياسات واضحة وشاملة عن كيفية حماية البيانات وان تطبقها. كما عليها ان تعين شخصا مسؤولا عن هذه الآليات وان تدرب موظفيها عليها وان تقيم عملياتها بشكل دوري. كما عليها تسجيل آلية معالجة البيانات. وتشمل هذه المعلومات اسم الشخص الذي اخذ البيانات والهدف من معالجتها ووصف لتصنيفها واذا ما ستتم مشاركتها مع اشخاص ثالثين وكيف سيتم نقلها وحمايتها ومتى سيتم اتلافها.

وبالتالي يقع على عاتق هذه الجهات مسؤولية الحفاظ على البيانات وعلى البنية التحتية التي تحويها. كما عليها ان تحقق في اي انتهاك وان تعلم السلطات المشرفة عليها والشخص المعني اذا ما حصل مثل هذه الانتهاكات.

وتشكل الرقابة عنصرا اساسيا للمساءلة. من هنا تتضمن معظم القوانين المتعلقة بجماية البيانات تحديد المسؤوليات للاشخاص المولجين بتجميع ومعالجة البيانات لضمان الامتثال بمعايير حماية البيانات.

يمكن ان يتضمن ذلك تعيين مسؤول حماية البيانات الذي يراقب وينظم تطبيق القانون.

وعلى هؤلاء المسؤولين ان يبلغوا عن اي خرق للبيانات في مهلة زمنية محددة وطبيعة الخرق والاشخاص المعنيين به والنتائج المترتبة والآليات الواجب اتخاذها لتخفيف الضرر. وقد عرفت ارشادات الاتحاد الاوروبي لحماية البيانات بخرق البيانات الشخصية في المادة الرابعة، بانه خرق للامن يؤدي بطريقة مقصودة او عرضية، الى تلف او ضياع او تشويه او نشر غير مصرح به او الوصول الى بيانات شخصية منقولة او محفوظة او قيد المعالجة.[50]

---

[50] Protection des données personnelles, Edition Legislatives, p.45

سادسا: الهيئة المشرفة المستقلة

من اجل حماية فعالة للحق الاساسي المتعلق بحماية البيانات الشخصية والمبادئ المترتبة عنه، يجب على التشريع ان يتضمن انشاء هيئة مشرفة مستقلة لديها مهام وصلاحيات واضحة وتنفيذية وتتوفر لها الاستقلالية. مهما كان شكل هذه الهيئة يجب ان يضمن القانون التالي :[51]

أ- في تشكيل الهيئة:

- يجب ان يتضمن القانون آلية تأسيس الهيئة وتعيين اعضائها ورئيسها.
- يجب ان يكون تكوينها وهيكليتها محددين بما فيه الخبرات المطلوبة.
- يجب ضمان اعطاء الهيئة الموارد المالية والبشرية والتقنية اللازمة.
- يجب ذكر ان الهيئة مستقلة وتبقى كذلك بهدف القيام بمهامها بتنفيذ اطار حماية البيانات بشكل فعال وكاف. يجب ان تبقى الهيئة حرة من اي تأثير خارجي وان تمتنع عن القيام باعمال لا تتناسب مع مهامها.
- يجب ان تمنح الهيئة مهام الرصد وتطبيق القانون، ما يتطلب مراجعات دورية للنشاطات التي تخضع للقانون.

ب- في مهام الهيئة:

- يجب ان تعطى الهيئة مهام تخولها القيام بتحقيقات والبت بالشكاوى عبر اصدار قرارات ملزمة وفرض عقوبات عندما تكتشف ان مؤسسة او جهاز ما قد خرق القانون. هذا يتضمن ان تكون الهيئة قادرة على طلب معلومات من الجهة التي تعالج البيانات، وان تقوم بتدقيق وبكافة

[51] دليل السياسات حول حماية الخصوصية، منظمة الخصوصية الدولية، ص ٨٦ - ٨٧
https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

الاجراءات التي تحتاجها لاستكمال التحقيق بما فيه معاينة المكان او المعدات التي تتم فيها معالجة البيانات.

- يجب ان تخول الهيئة قبول الشكاوى والاستجابة لها ان من الافراد او من الجمعيات الخاصة ذات المصلحة العامة. كما يجب ان تخول النظر في الشكاوى حول ممارسات سيئة قبل حصول انتهاك معين اذا ما كان هناك اثبات على هذه الممارسات.
- على الهيئة ان يكون لديها استشارية حيث يمكن للاجهزة الحكومية والادارية ان تطلب المشورة فيما يتعلق بحماية حقوق الافراد وحرياتهم المتعلقة بمعالجة بياناتهم الشخصية.
- على الهيئة ان توفر المعلومات للافراد الذين يريدون معلومات عن بياناتهم الشخصية.
- للهيئة مهام تعزيز وعي الافراد العام وذلك كجزء من دورها في ترسيخ فهم الافراد لحقوقهم المتعلقة ببياناتهم الشخصية والمخاطر الناجمة عن معالجتها وطرق حمايتها.

ج- في الصلاحيات الممنوحة للهيئة:

- يجب ان تعطى الهيئة صلاحية فرض العقوبات بما فيها الغرامات والانذارات والتعهدات والملاحقة. هذه الصلاحية لا يجب ان تكون مربوطة بشكوى من المتضرر صاحب البيانات بل يمكن فرضها تلقائيا من الهيئة.
- لدى الهيئة صلاحية اصدار توصيات وارشادات لتفسير بعض مواد قانون حماية البيانات اما بشكل عام او لجهة معينة ما. هذا الامر يجعل من القانون قابلا لمحاكاة التطور التكنولوجي السريع الذي يحصل.
- يمكن اعطاء الهيئة بعض الصلاحيات التنظيمية بمعنى تحديث بعض جوانب القانون مثل التعريفات وموجبات الامان والموافقة على تدفق البيانات العابر للحدود.

المبحث الثاني: القوانين اللبنانية الحالية التي تحمي البيانات الشخصية:

في اطار التزام لبنان بالوفاء بالالتزامات الدولية وبمراعاة المعايير الدولية التي تفرضها حماية الخصوصية والبيانات الشخصية ومجاراة مع المنحى الرقمي الذي تتجه اليه الادارة اللبنانية وكافة الاجهزة الامنية، ومع تزايد جمع البيانات من مختلف الجهات العامة والخاصة، يقتضي وجود قوانين ترعى ضمان حماية البيانات الشخصية. يشكل هذا الامر اولوية وعلى الحكومة اللبنانية ان تتعاطى بشفافية مع الموضوع كما على المشرع اللبناني توفير المنظومة القانونية الضرورية لحماية هذا الحق.

في ضوء العديد من التقارير التي اشارت الى استخدام بعض الاجهزة اللبنانية أدوات تجسس متطّورة ما يشّكل تهديداً مباشراً لخصوصية المواطنين اللبنانيين، وفي ضوء الحديث عن حكومة الكترونية في خطط الوزارات المتعاقبة وبدء بعض الاجهزة بالرقمنة لاسيما الامن العام الذي بدأ باعتماد جوازات السفر البيومترية، كل ذلك يقتضي البحث اذا ما كانت الاطر القانونية الموجود حاليا كافية لترعى كل هذه الجوانب وما اذا كانت تتضمن معايير قوية لحماية البيانات وكيفية تخزينها ومعالجتها وضمان سلامتها. لذا نستعرض في هذا المبحث القوانين اللبنانية التي تتضمن موادا تتعلق بالبيانات الشخصية لاسيما قانون الاتصالات وبعض القوانين المتعلقة بمنع افشاء الاسرار وصولا الى قانون الوصول الى المعلومات. ومن ثم نخصص المطلب الثاني لشرح قانون المعاملات الالكترونية وحماية البيانات الشخصية ومدى مطابقته للمعايير الدولية.

المطلب الاول: القوانين اللبنانية التي تتضمن موادا تتعلق بالبيانات الشخصية

قبل اقرار قانون المعاملات الالكترونية وحماية البيانات الشخصية رقم ٨١، تاريخ ٢٠١٨/١٠/١٠ لم يكن هناك اطار قانوني خاص بحماية البيانات الشخصية انما كنا نجد موادا مبعثرة في نصوص مختلفة تتحدث عن خصوصية البيانات الشخصية وحمايتها وسنستعرضها في هذا المطلب وأهمها قانون الاتصالات رقم ١٤٠ الذي ضمن حماية بيانات الاتصالات عبر آليات محددة وقوانين اخرى مثل قانون السرية المصرفية

وقانون العقوبات وبعض قوانين تنظيم المهن وقانون حماية المستهلك وآخرها قانون الوصول الى المعلومات الذي اقر في ٢٠١٧. سنستعرض هذه النصوص لجهة ما تضمنه من بيانات تتعلق بحماية البيانات الشخصية.

اولا: قانون الاتصالات

يعتبر لبنان من البلدان الاولى على المستوى العربي الذي أدخل اطارا قانونيا لاعتراض الاتصالات [52] عبر قانون الاتصالات رقم ٩٩/١٤٠ وقد خصصنا جزءا من دراستنا في الفصل الاول لهذا القانون الذي يقيد اي خرق للخصوصية عبر التنصت او الرصد او الاعتراض او الكشف الا في حالات الضرورة وبعد الحصول على امر قضائي او اداري بحالات مفصلة في القانون ووفق آليات محددة. كما شرحنا سابقا فان الحصول على اذن قضائي للحصول على بيانات الاتصالات او اعتراضها يعطى بموجب قرار من المحكمة شرط ان يكون الشخص المستهدف هو المشتبه بارتكابه جريمة وان يحدد امر المحكمة وسائل الاتصال وموضوع الاجراء والسبب اي الجريمة قيد التحقيق ومدة الاعتراض التي لا يمكن ان تتجاوز الشهرين. اما الاعتراض الاداري فيحصل اما من وزير الداخلية او وزير الدفاع بعد الحصول على موافقة رئيس مجلس الوزراء من اجل جمع معلومات تهدف الى مكافحة الارهاب او حول جرائم ضد امن الدولة، على ان تكون الموافقة خطية ومبررة وبموافقة رئيس مجلس الوزراء. وايضا يجب ان تحدد وسائل الاتصال وموضوع الاجراء والجريمة موضوع التحقيق ومدة الاعتراض على ان لا تتجاوز الشهرين. وتتحقق من القرارات الادارية لجنة قضائية مستقلة. اذا يوفر القانون اللبناني ضمانات لجهة حماية بيانات الاتصالات لاسيما في الاعتراض الاداري وربطه بهيئة قضائية مستقلة مولجة بالاشراف على التفويض الاداري. الا ان المشكلة

[52] التقرير الدوري الشامل حول حق الخصوصية في لبنان مقدم من منظمة تبادل الاعلام الاجتماعي والخصوصية الدولية وجمعية الاتصالات التقدمية الى مجلس حقوق الانسان، https://www.upr-lebanon.org/wp-content/uploads/2015/11/289002529.pdf

في لبنان تكمن في الممارسة عبر تعطيل الهيئات المشرفة المستقلة او القضائية وسنورد مثالا على تخطي السلطة القضائية والاكتفاء بالتفويض السياسي لرئيس مجلس الوزراء وذلك في قضية "داتا الاتصالات".

ثانيا: القوانين المتعلقة بمنع افشاء الاسرار

هنالك بعض القوانين التي تتعلق بتنظيم المهن والقطاعات والتي تمنع افصاح البيانات الشخصية الموجودة في حوزتهم.

من هذه القوانين قانون سرية المصارف الصادر عام ١٩٥٦ [53] والذي ينص في مادته الثانية على ان كل من له اطلاع بحكم صفته او وظيفته باية طريقة على قيود الدفاتر والمعاملات والمراسلات المصرفية يلزمون بكتمان السر اطلاقا لمصلحة الزبائن ولا يجوز لهم افشاء ما يعرفونه عن اسماء الزبائن واموالهم والامور المتعلقة بهم لاي شخص فردا كان ام سلطة عامة ادارية او عسكرية او قضائية الا اذا اذن لهم بذلك خطيا صاحب الشأن او ورثته او الموصى لهم او اذا اعلن افلاسه او اذا نشأت دعوى تتعلق بمعاملة مصرفية بين المصارف وزبائنها. كذلك اكملت المادة الثالثة على حق المصارف بفتح حسابات ودائع مرقمة لزبائنها لا يعرف اصحابها غير المدير او وكيله ولا تعلن هوية صاحب الحساب المرقم الا باذنه الخطي. هذه السرية للبيانات تستثني فقط الطلبات القضائية في دعاوى الاثراء غير المشروع حسب المادة السابعة.

اما قانون العقوبات [54] فينص في المواد ٥٧٩ الى ٥٨١ على ما يتعلق بافشاء الاسرار، ويمنع من كان بحكم وضعه او وظيفته او مهنته او فنه وقد علم بسر، افشاءه دون سبب شرعي او استخدامه لمنفعة خاصة تحت طائلة عقوبة حبس سنة على الاكثر. كذلك يعاقب بالحبس من شهرين الى سنتين كل شخص ملحق بمصلحة البريد يسيء استعمال صفته ليطلع على رسالة مختومة او يتلف او يختلس احدى الرسائل او يفضي بمضمونها لغير المرسل له. ونفس الامر لمن كان ملحقا بمصلحة الهاتف.

---

[53] نص قانون سرية المصارف: https://cyrilla.org/ar/entity/vj24q5xwaxx1hhm4h48b5u3di?page=1

[54] نص قانون العقوبات اللبناني:
http://www.legallaw.ul.edu.lb/LawView.aspx?opt=view&LawID=244611#Section_260398

كما تنص المادة ٤٢٠ من قانون العقوبات على ما يحظر نشوه من بيانات وضمنها وثيقة من وثائق التحقيق الجنائي أو الجناحي قبل تلاوتها في جلسة علنية، مذكرات المحاكم، محاكمات الجلسات السرية، المحاكمات في دعوى نسب، المحاكمات في دعوى الطلاق أو الهجر، كل محاكمة منعت المحاكم نشرها.

اما قانون حماية المستهلك رقم ٦٥٩ الصادر في ٤ شباط ٢٠٠٥ فقد تضمن مادتين ٥١ و٥٨ نصتا على أنه يجب ألا يفصح المزّودون عن البيانات عنها دون موافقة المستهلكين.

على صعيد آخر تنظم بعض القوانين المهن وتتضمن حماية سرية المهنة مثل قانون الآداب الطّبية رقم 288 الصادر في ٢٢ شباط ١٩٩٤ الذي يحمي سّرية العلاقة بين الطبيب والمريض.

ثالثا: قانون الوصول الى المعلومات

شكّل اقرار قانون الحق في الوصول الى المعلومات في لبنان رقم ٢٨ الصادر في شباط ٢٠١٧ خطوة كبيرة على صعيد تطوير القوانين اللبنانية من أجل تعزيز دولة القانون واعتماد مبادئ الشفافية في إدارة الشأن العام ومواكبة طروحات الاصلاح ومكافحة الفساد، وذلك من خلال تمكين المواطنين والجمعيات والصحافيين من الوصول الى مصادر المعلومات والزام الادارات العامة بالعلنية في كل انشطتها وقراراتها، وذلك بغض النظر عن فعالية تطبيقه اليوم والتعاطي السلبي معه عموما من جانب الادارة اللبنانية اما يعيق تفعيله .[55]

وشكل اقرار هذا القانون في لبنان خطوة مهمة لتعزيز الشفافية في الادارة العامة ان عبر النشر الحكمي الذي تضمنه او عبر الاتاحة لاي مواطن طلب الوصول الى المعلومات من اية ادارة عامة. وكان لبنان قد انضم الى اتفاقية مكافحة الفساد الصادرة عام ٢٠٠٣ والتي تكرس هذا الحق في نيسان ٢٠٠٩. نورد هذه الاتفاقية كاطار عام للمعايير الدولية والتي تضمنت تشديدا على حماية البيانات الشخصية في موضوع

[55] قانون الحق في الوصول الى المعلومات: دراسة تقييمية عن تطبيقه واستخداماته، مؤسسة مهارات، نشرت في شباط ٢٠٢٠ http://maharatfoundation.org/media/1783/access-study-2020.pdf

الحصول على المعلومات من الادارة. اذ شددت على اعتماد إجراءات أو لوائح تمكن عامة الناس من الحصول، عند الاقتضاء، على معلومات عن كيفية تنظيم الادارة العمومية والية عملها وعمليات اتخاذ القرارات فيها، وعن القرارات والصكوك القانونية التي تهم عامة الناس، مع ايلاء المراعاة الواجبة لاحترام خصوصيتهم وحماية بياناتهم الشخصية.

وقد جسد فعلا قانون حق الوصول الى المعلومات الالتزامات والحقوق المنصوص عنها في اتفاقية مكافحة الفساد. ونشير هنا لاهمية هذا القانون لناحية تضمينه الحق في حماية المعلومات الشخصية وتصحيحها وتحديثها ومحوها.

اذا القى هذا القانون [56] موجبا مهما على عاتق الادارات العامة بحماية البيانات الشخصية وتولية اصحابها حقوقا عليها. وعرفت المادة الثانية من القانون الادارة العامة ب:

1. الدولة وإداراتها العامة.
2. المؤسسات العامة.
3. الهيئات الادارية المستقلة.
4. المحاكم والهيئات والمجالس ذات الطابع القضائي او التحكيمي، العادية والاستثنائية، بما فيها المحاكم العدلية والادارية والمالية دون المحاكم الطائفية.
5. البلديات واتحادات البلديات.
6. المؤسسات والشركات الخاصة المكلفة بإدارة مرفق او ملك عام.
7. الشركات المختلطة.
8. المؤسسات ذات المنفعة العامة.

[56] نص قانون الوصول الى المعلومات:
http://www.legiliban.ul.edu.lb/LawView.aspx?opt=view&LawID=269965

9. سائر اشخاص القانون العام.

10. الهيئات الناظمة للقطاعات لا سيما هيئة إدارة النفط والصندوق السيادي والصناديق الأخرى.

وفصلت المادة الرابعة الحقوق المترتبة لصاحب العلاقة فيما يتعلق بالمستندات الادارية المتعلقة بمعلومات ذات طابع شخصي واعتبرت انه "يحق لصاحب العلاقة دون سواه الوصول الى الملفات الشخصية وأي تقرير تقييمي يتعلق بشخص طبيعي مشار إليه بالاسم أو برقم تعريفي أو برمز أو بأي وصف تعريفي آخر كبصمات الاصابع او العين او الصوت او الصورة." كما تابعت تعريف الملفات الشخصية على انها "قيود الاحوال الشخصية والملفات التي تتضمن جميع أنواع المعلومات المتعلقة بالشخص الطبيعي على نحو مباشر أو غير مباشر. بما في ذلك عنوان بروتوكول الانترنت (IP address) وذلك عن طريق مقارنة المعلومات المتعددة المصادر أو التقاطع فيما بينها." كما رسخت لصاحب العلاقة حقوقا على بياناته اذ "يحق لصاحب العلاقة الطلب لتصحيح أو اكمال او تحديث او محو المعلومات الشخصية المتعلقة به غير الصحيحة او الناقصة او الملتبسة او القديمة أو التي يكون من الممنوع جمعها أو استعمالها أو تبادلها أو حفظها."

كما ان المادة ٥ وفي اطار تعدادها للمستندات غير القابلة للاطلاع شددت في النقطة الرابعة من الفقرة أ على انه لا يمكن الوصول الى المعلومات المتعلقة بحياة الافراد الخاصة وصحتهم العقلية والجسدية اضافة الى الاسرار التي يحميها القانون كالسر المهني او السر التجاري مثلا. كما ان الفقرة ب من المادة الخامسة نصت في النقطة الاولى انه لا يمكن الاطلاع على وقائع التحقيقات قبل تلاوتها في جلسة علنية، والمحاكمات السرية، والمحاكمات التي تتعلق بالأحداث وبالأحوال الشخصية. كما منعت المادة ٢٠ اعادة استخدام المعلومات في سبيل غايات تجارية الا اذا جمعت ضمن مضمون مبتكر مع احترام قانون حماية الملكية الادبية والفنية على الا تتضمن المستندات المذكورة اي معلومات ذات طابع شخصي ومع مراعاة حقوق الملكية الفكرية.

وبذلك يكون قانون الوصول الى المعلومات قد تضمن للمرة الاولى اطارا عاما لمبدأ حماية البيانات الشخصية المتواجدة في حوزة الادارة وعرفها واعطى اصحابها حقوقا عليها وفرض الادارة مراعاة حمايتها وعدم الكشف عنها. ولكن يبقى هذا الاطار عاما لا يؤمن حماية فعالة للبيانات الشخصية بحسب المعايير الدولية التي ذكرناها سابقا لاسيما لجهة نقص تفاصيل آلية الحماية وموجبات الادارة ورضى صاحب البيانات والهيئة المستقلة للاشراف على احترام الادارات لموجب حماية البيانات.

المطلب الثاني: قانون المعاملات الالكترونية وحماية البيانات الشخصية

يأتي اليوم البحث في الاطار القانوني الجديد الذي وضعه القانون رقم ٨١ في ١٠-١٠- ٢٠١٨ لحماية البيانات الشخصية ليثير الكثير من التساؤلات حول مدى تلاؤم هذا الاطار مع المعايير الدولية لحماية البيانات. ويقتضي استعراض مسار هذا القانون التشريعي لاسيما مع البطء التشريعي الذي نعاني منه في لبنان. هذا البطء الذي يبعد في بعض الاحيان مضامين القوانين عن الغاية المرجوة منها اذا ما تم اقراره بعد عشر سنوات مثلا، وخاصة اذا كان مرتبطا بالتطورات التكنولوجية التي لا تستطيع برلمانات العالم الاكثر تطورا وفعالية وديمقراطية اليوم مواكبتها. وان موضوع حماية البيانات من اكثر المواضيع ارتباطا بالتطور التكنولوجي والرقمي مع دخولنا اليوم في عصر الـ"بيغ داتا". توثق دراسة حرية الانترنت لمؤسسة مهارات المنشورة في العام ٢٠١٥ [57] والدراسة المحدثة المنشورة في ٢٠١٨، مسار قانون المعاملات الالكترونية وحماية البيانات الشخصية الذي لا يدل الا على غياب تصور كامل لدى المشرع اللبناني لحماية المحتوى الرقمي والبيانات الشخصية.

بدأت لجنة تكنولوجيا المعلومات في المجلس النيابي اللبناني بدراسة إقتراح قانون المعاملات الالكترونية منذ العام ٢٠٠٤ ولم يتم اقراره بصيغته الاولية حتى ايلول من العام ٢٠١٠ وذلك من قبل اللجنة الفرعية

[57] دراسة حرية الانترنت، مؤسسة مهارات، ٢٠١٥، ص ٤١
http://maharatfoundation.org/media/1639/حرية-الانترنت-في-لبنان.pdf

المنبثقة عن اللجان المشتركة. وفي ١٧ آب من العام ٢٠١١ قررت الهيئة العامة لمجلس النواب سحب الاقتراح المتعلق باحكام المعاملات الإلكترونية من جدول اعمال الهيئة العامة ريثما تقدم الحكومة مشروعاً متكاملاً بالخصوص .

واعادت الحكومة تقديم مشروع جديد في تشرين الاول ٢٠١٢ بإسم "مشروع قانون المعاملات الالكترونية والبيانات ذات الطابع الشخصي" احيل الى المجلس النيابي بموجب المرسوم رقم ٩٣٤١ واستكملت اللجنة الفرعية المنبثقة عن اللجان النيابية المشتركة في ١٠ نيسان ٢٠١٥ دراسة هذا المشروع لإقراره وانتهت من مناقشته في ١٤ آذار ٢٠١٨ لتحيله الى الهيئة العامة لتقره الاخيرة في ١٠ تشرين الاول ٢٠١٨.

اولا: المبادئ التي يرسخها قانون المعاملات الالكترونية وحماية البيانات الشخصية

تضمنت الاسباب الموجبة للقانون اعترافا بان المعاملات الالكترونية في لبنان اصبحت واقعًا يوميًا، الا انها تتم في ظل فراغ تشريعي، اذ ان القوانين اللبنانية المعمول بها عاجزة عن مجاراة التطور الحاصل وايجاد الحلول القانونية الملائمة. من هنا أتى هذا القانون للاعتراف بالاسناد الاالكترونية والتواقيع الالكترونية واعتماد الاثبات الالكتروني، فضلا عن تنظيم القطاع المتعلق بالتجارة الالكترونية والمعاملات الالكترونية وتقديم خدمات الاتصال ومنح اسماء المواقع المتعلقة بالنطاق الوطني lb.. ما يهمنا من القانون ما تضمنته اسبابه الموجبة حول انه اصبح ايضاً من الضروري تنظيم معالجة البيانات ذات الطابع الشخصي وتطبيق ضوابط قانونية في هذا المجال، مراعاة لخصوصية الفرد وحرياته الشخصية. واتى الباب الخامس ايضا حسب الاسباب الموجبة ليضع تنظيماً قانونياً متكاملاً لموضوع حماية البيانات ذات الطابع الشخصي. فهو يحدد اهداف معالجة المعلومات ذات الطابع الشخصي وضوابطها والمعالجات الممنوعة قانوناً وكيفية جمع المعلومات ذات الطابع الشخصي وموجبات المسؤول عن المعالجة ومسؤولياته. كما يورد هذا الباب لائحة طويلة من المعالجات المعفية من التصريح او طلب الترخيص لوضعها قيد التنفيذ. وينظم بالمقابل اصول التصريح عن المعالجات غير المعفية او طلب الترخيص بخصوص بعضها من المرجع الرسمي المختص.

كما ينص الباب الخامس على حقوق قانونية للشخص الذي تتعلق به البيانات موضوع المعالجات: حقه في الاعتراض على هذه المعالجات، حقه في الاستعلام عن هذه المعالجات، وطلب معلومات بشأنها، حقه في طلب تصحيح المعلومات المتعلقة به او تحديثها او اكمالها او محوها...

ونظرا لاهمية هذا الاطار القانوني المستحدث سنستعرض ابرز المبادئ التي كرسها في بابه الخامس [58] ومدى مطابقتها مع المعايير الدولية لاسيما لائحة الاتحاد الاوروبي لحماية البيانات الشخصية.

تعرف المادة الاولى من القانون بالمصطلحات المتعلقة بالبيانات الشخصية كالتالي:

- مستضيف البيانات:(Hébergeur de données/Data host) هو من يقوم بتخزين المعلومات أياً تكن طبيعتها، لحساب الغير، مقابل عوض أو دون عوض، ويضعها في متناول الجمهور من خلال خدمات الاتصال المباشر.
- المعلومات المتعلقة بحركة البيانات Données de trafic/ Traffic data: هي أية معلومات متعلقة بعملية إتصال بواسطة نظام حاسب آلي مرتبط بشبكة معلوماتية. تصدر هذه المعلومات عن نظام حاسب آلي مرتبط بالشبكة، وتدل على مصدر الإتصال ومتلقيه وخط سير المعلومات والوقت والتاريخ والحجم والمدة الزمنية أو ما شابه ذلك من المعلومات.
- البيانات ذات الطابع الشخصي Données à caractère personnel/Personal Data: هي جميع أنواع المعلومات المتعلقة بشخص طبيعي التي تمكن من التعريف به، على نحو مباشر أو غير مباشر، بما في ذلك عن طريق مقارنة المعلومات المتعددة المصادر أو التقاطع فيما بينها.
- معالجة البيانات ذات الطابع الشخصي Traitement des Données à caractère personnel /Processing of Personal Data: هي كل عملية أو مجموعة عمليات تقع على هذه البيانات

[58] نص قانون المعاملات الالكترونية وحماية البيانات الشخصية: https://www.lp.gov.lb/Resources/Files/f67b348c-6d35-42a0-8ddb-c18bcc2a5e8d.pdf

مهما كانت الوسيلة المستخدمة،لاسيما عمليات التجميع والتسجيل والتنظيم والحفظ والتكييف والتعديل والإقتطاع والقواءة والإستعمال والنقل والنسخ والنشر والمحو والإتلاف وكل شكل آخر لوضع المعلومات تحت التصرف.

- صاحب البيانات ذات الطابع الشخصي: (المعروف أيضاً بالشخص المعني بالبيانات ذات الطابع الشخصي) هو الشخص الطبيعي الذي تتعلق به هذه البيانات.
- المسؤول عن معالجة البيانات ذات الطابع الشخصي: هو الشخص الطبيعي أو المعنوي الذي يحدد أهداف المعالجة وأساليبها.
- أُلموسل إليه البيانات ذات الطابع الشخصي: هو الشخص أُلمخول استلام البيانات ذات الطابع الشخصي، وهو غير الشخص المعني بالمعالجة أو المسؤول عن المعالجة أو من ينخوها. لا تعتبر بحكم أُلموسل إليه السلطات العامة المخولة قانوناً ضمن مهامها طلب بيانات ذات طابع شخصي.

وضعت المادتان ٨٥ و٨٦ احكاما عامة على نطاق تطبيق هذا الباب لتشمل جميع المعالجات الآلية وغير الالية للبيانات ذات الطابع الشخص، لكنها لا تطبق على المعالجات المتعلقة بالنشاطات الشخصية التي يقوم بها الشخص حصريا لحاجاته.ولا يمكن الاتفاق على عكس المبادئ التي تضمنها القانون في تنظيم حقوق الاشخاص المعنيين وموجبات المسؤولين عن معالجة البيانات. كما رسخت الاحكام العامة في هذا الباب حق كل شخص في الاطلاع والاعتراض امام المسؤول عن معالجة البيانات على المعلومات والتحاليل المستعملة في المعالجات.

اما الفصل الثاني من الباب الخامس فيضع اصولا محددة لتجميع المعلومات ذات الطابع الشخصي ومعالجتها. وتحدد المادة ٨٧ ان البيانات ذات الطابع الشخصي تجمع بأمانة ولأهداف مشروعة ومحددة وصريحة. ويجب ان تكون البيانات ملائمة وغير متجاوزة للاهداف المعلنة، وان تكون صحيحة وكاملة وان

تبقى محدثة بالقدر اللازم.ولا يمكن في مرحلة لاحقة معالجة هذه البيانات لأهداف لا تتوافق مع الغايات المعلنة، ما لم يتعلق الامر بمعالجة بيانات لأهداف احصائية او تاريخية او للبحث العلمي.

وتضع المادة ٨٨ موجب الاعلام على عاتق المسؤول عن معالجة البيانات ذات الطابع الشخصي او ممثله فيما يتعلق بهوية المسؤول عن المعالجة او هوية ممثله، اهداف المعالجة، الطابع الالزامي او الاختياري للاجابة على الاسئلة المطروحة، النتائج التي قد تترتب على عدم الاجابة، الاشخاص الذين سترسل اليهم البيانات، حق الوصول الى المعلومات وتصحيحها والوسائل المعدة لذلك، على ان تكون هذه المعلومات كلها واردة في الاستمارات المستعملة لجمع البيانات. وحتى ان المادة ٨٩ تشدد على ابلاغ الشخص الذي تطلب منه البيانات بكل هذه المعلومات ولو كانت البيانات تجمع منه وهو غير معني بها. واضافت المادة ٩٠ ان حفظ البيانات لا يكون مشروعا الا خلال الفترة المبينة في التصريح عن المعالجة ومنعت المادة ٩١ جمع البيانات اذا كانت تكشف بصورة مباشرة او غير مباشرة، عن الحالة الصحية او الهوية الوراثية او الحياة الجنسية للشخص المعني، الا في حالات محددة هي:

- عندما يكون الشخص المعني قد وضع هذه البيانات في متناول الجمهور اووافق صراحةً على معالجتها، ما لم يوجد مانع قانوني.
- عندما يكون تجميع البيانات او معالجتها ضروريين لوضع تشخيص طبي او تقديم علاج طبي من قبل عضو في مهنة صحية.
- عند اثبات حق او الدفاع عنه امام القضاء.
- في حال الحصول على ترخيص وفق احكام المادة 97 من هذا القانون.

واعطت المادة ٩٢ لكل شخص طبيعي الحق في الاعتراض لأسباب مشروعة، امام المسؤول عن المعالجة على تجميع البيانات ذات الطابع الشخصي الخاصة به ومعالجتها، بما في ذلك التجميع والمعالجة لهدف الترويج التجاري، الا اذا كان المسؤول عن معالجة البيانات ملزماً بجمعها بمقتضى القانون او اذا كان قد

وافق على معالجة البيانات ذات الطابع الشخصي الخاصة به. وضمنت المادة ٩٣ موجب حماية البيانات عبر الزام المسؤول عن معالجة البيانات ذات الطابع الشخصي باتخاذ جميع التدابير، في ضوء طبيعة البيانات والمخاطر الناتجة عن المعالجة، لضمان سلامة البيانات وامنها ولمنع تعرضها لتشويه او تضررها او وصولها الى اشخاص غير مخولين الاطلاع عليها.

اما الفصل الثالث فنص على الاجراءات المطلوبة لوضع المعالجات قيد التنفيذ. وسمحت المادة ٩٤ عدم وجوب اي تصريح او طلب اي ترخيص لمعالجة بيانات ذات طابع شخصي في الحالات التالية:

1. في المعالجات التي يجريها اشخاص الحق العام كل في نطاق صلاحياته.
2. في حال قيام جمعيات لا تبغي الربح، بمسك السجلات الخاصة بأعضائها والمتعاملين معها ضمن نطاق ممارستها بشكل طبيعي وقانوني لمهامها.
3. في المعالجات التي يكون موضوعها مسك سجلات مخصصة، بموجب احكام قانونية او تنظيمية، لاعلام الجمهور والتي يمكن ان يطلع عليها كل شخص او اشخاص لهم مصلحة مشروعة.
4. في المعالجات التي يكون موضوعها التلاميذ والطلاب من قبل المؤسسات التربوية لغايات تربوية او ادارية خاصة بالمؤسسة.
5. في المعالجات التي يكون موضوعها الاجراء او الاعضاء في المؤسسات والشركات التجارية والنقابات والجمعيات واصحاب المهن الحرة، وذلك في حدود ولحاجات ممارسة نشاطاتهم بشكل قانوني.
6. في المعالجات التي يكون موضوعها الزبائن والمتعاملين مع المؤسسات والشركات التجارية والنقابات والجمعيات واصحاب المهن الحرة، وذلك في حدود ولحاجات ممارسة نشاطاتهم بشكل قانوني.
7. اذا وافق الشخص المعني مسبقاً على معالجة بياناته الشخصية ما لم يوجد مانع قانوني.

8. يمكن ايضاً اعفاء بعض المعالجات او بعض فئاتها من اجراءات التصريح او الترخيص اذا تبين ان وضعها قيد التنفيذ لا يستتبع اي خطر يهدد الحياة الخاصة او الحريات الشخصية، وذلك بموجب مرسوم يتخذ في مجلس الوزراء بناءً على اقتراح وزيري العدل والاقتصاد والتجارة.

9. في المعالجات المنصوص عنها في القانون رقم 140/99 وضمن حدوده.

وأوجبت المادة ٩٥ في غير الاعفاءات المنصوص عليها في المادة ٩٤ على من يرغب بجمع البيانات ذات الطابع الشخصي ومعالجتها، اعلام وزارة الاقتصاد والتجارة بموجب تصريح وفق الاصول لقاء ايصال. على ان يتضمن هذا التصريح حسب المادة ٩٦ غايات المعالجة، البيانات ذات الطابع الشخصي موضوع المعالجة ومصدرها، فئات الاشخاص المعنيين، الاشخاص الثالثين او فئاتهم الذين يمكن اطلاعهم على البيانات، مدة الاحتفاظ بالبيانات، هوية وعنوان المسؤول عن المعالجة ولو كان هذا المسؤول مقيماً خارج الاراضي اللبنانية، الجهاز او الاجهزة المكلفة وضع المعالجة قيد التنفيذ، الشخص او الجهاز الذي يمارس لديه حق الوصول وكيفية ممارسته، المتلزم من الباطن او المقاول الثانوي في حال وجوده، وعند الاقتضاء، طرق الوصل او اي شكل آخر من الربط بين البيانات وبين معالجات اخرى اضافة الى التنازلات الممكنة عن البيانات للغير وايضا عند الاقتضاء، نقل البيانات ذات الطابع الشخصي الى دولة اخرى في اي شكل كان، الاجراءات المتخذة لضمان سلامة البيانات ذات الطابع الشخصي وضمان حفظ الاسرار المحمية بموجب القانون، والتي يقع موجب تنفيذها السليم على عاتق المسؤول عن المعالجة، والتأكيد على ان المعالجة سوف تتم وفقاً للقانون.

كما نصت المادة ٩٧ على وجوب استحصال ترخيص لمعالجة البيانات المتعلقة بالامن الخارجي والداخلي للدولة بموجب قرار مشترك يصدر عن وزيري الدفاع الوطني والداخلية والبلديات، او بالجرائم الجزائية وبالدعاوى القضائية بمختلف انواعها بموجب قرار يصدر عن وزير العدل او بالحالات الصحية او بالهوية الوراثية او بالحياة الجنسية للاشخاص بموجب قرار يصدر عن وزير الصحة العامة. على ان يصدر قرار

الترخيص ضمن مهلة شهرين والا اعتبر مرفوضا ضمنا، ويبلغ في الحالتين خطيا الى وزارة الاقتصاد والتجارةوالى مقدم الطلب. على ان تضع بحسب المادة ٩٨ وزارة الاقتصاد في متناول الجمهور على موقعها لائحة بالمعالجات الممكننة التي استوفت اجراءات الترخيص او التصريح مع تفاصيل المعالجة لناحية تاريخ اعطاء الترخيص وتاريخ البدء بالمعالجة والغاية منها وهوية وعنوان المسؤول عنها وفئات البيانات والشخص او الادارة التي يمارس لديها حق الوصول الى البيانات والاشخاص الثالثين المخولين الاطلاع عليها وعند الاقتضاء البيانات المنوي نقلها الى دولة اجنبية.

اما الفصل الرابع من الباب الخامس فيكرس حق الوصول والتصحيح وتتيح المادة ٩٩ لكل صاحب بيانات ذات طابع شخصي او لأي من ورثته الحق في الاستعلام من المسؤول عن معالجة البيانات لمعرفة ما اذا كانت هذه البيانات الخاصة به موضوع معالجة ام لا. وعلى هذا المسؤول ان يسلم صاحب البيانات نسخة عن البيانات العائدة له بناءً على طلبه. اذا كانت هذه البيانات مرمزة او مضغوطة او مشفرة فيجب ان يُعطى صاحب البيانات ذات الطابع الشخصي او لأي من ورثته نسخة مفهومة. كما لصاحب البيانات او لأي من ورثته ان يطلب ايضاً من المسؤول عن معالجتها تسليمه المعلومات الاضافية المتعلقة بغايات المعالجة، فئاتها، مصدرها، موضوع المعالجة وطبيعتها، تحديد الاشخاص وفئاتهم الذين ترسل اليهم البيانات ذات الطابع الشخصي او الذين يمكنهم الاطلاع عليها ومواقيتها وغايات هذا الاطلاع. ونصت المادة ١٠٠ على امكانية ان يستوفي المسؤول عن المعالجة بدلا لقاء اعطاء نسخة عن البيانات على ان لا يتعدى البدل كلفة النسخ. كما اعطته المادة ١٠٠ حق الاعتراض على الطلبات ذات الطابع التعسفي، لا سيما في ما خص عددها او طابعها المتكرر او المنهجي، على ان يقع عليه عبء اثبات تعسفية الطلب. واعطت المادة ١٠١ لصاحب البيانات حق طلب تصحيحها واكمالها وتحديثها ومحوها، والتي تكون غير صحيحة او ناقصة او ملتبسة او منتهية الصلاحية او غير متوافقة مع غايات المعالجة او تلك الممنوع معالجتها او جمعها او استخدامها او حفظها او نقلها. وعلى مسؤول المعالجة اذا ما كانت البيانات ارسلت الى شخص

ثالث ان يبلغه بالتصحيح. على ان يقوم بالعمليات المطلوبة مجانا في مهلة عشرة ايام من تقديم طلب التصحيح ومع القاء موجب التصحيح التلقائي على عاتق مسؤول المعالجة عندما يأخذ علماً بأحد الاسباب التي تلزمه بتعديلها او الغائها. ولصاحب البيانات وفق المادة ١٠٢ مراجعة المحاكم المختصة، لا سيما قاضي الامور المستعجلة لضمان ممارسة حق الوصول والتصحيح. واستثنت المادة ١٠٣ الحالات التي لا يمكن لصاحب البيانات الاطلاع عليها وهي عندما تتعلق المعالجات بأمن الدولة الداخلي او الخارجي اذا كان ذلك يعرض غاياتها او امن الدولة الداخلي او الخارجي للخطر. اما المادة ١٠٤ فقد اخضعت حق الافراد في الوصول الى السجلات والملفات العامة والملفات الطبية التي تحتوي على بيانات ذات طابع شخصي للاحكام القانونية والتنظيمية التي ترعاها. واضافت ان معالجة البيانات ذات الطابع الشخصي وحق الوصول اليها وتصحيحها في الوزارات والادارات والمؤسسات العامة خارج اطر النصوص القانونية والتنظيمية الخاصة بها تخضع لاحكام هذا القانون ولترخيص مسبق يصدر عن مجلس الوزراء بناءً لاقتراح الوزير المختص. واستثنت المادة ١٠٥ حق صاحب البيانات بالوصول اليها وتصحيحها اذا كانت معالجتها تتم فقط لغايات التعبير الادبي والفني او لغايات الممارسة المهنية لنشاط صحافي في حدود التقيد بالقوانين النافذة. وتضمن الفصل الخامس والاخير من الباب الخامس احكاما جزائية يعاقب من خلالها في المادة ١٠٦ بالغرامة وبالحبس كل من اقدم على معالجة بيانات ذات طابع شخصي دون تقديم تصريح، او دون الاستحصال على ترخيص مسبق قبل المباشرة بعمله وفقاً لاحكام الفصل الثالث من هذا الباب، وكل من اقدم على جمع او معالجة بيانات ذات طابع شخصي دون التقيد بالقواعد المقررة وفق احكام الفصل الثاني من هذا الباب، وكل من اقدم، ولو بالاهمال، على افشاء معلومات ذات طابع شخصي موضوع معالجة لاشخاص غير مخولين الاطلاع عليها. كما تعاقب المادة ١٠٧ بالغرامة كل مسؤول عن معالجة بيانات ذات طابع شخصي رفض الاجابة في مهلة عشرة ايام عمل، او اجاب بصورة غير صحيحة او ناقصة على طلب الشخص المعني بالمعالجة او وكيله في شأن حق الاطلاع او التصحيح. ذلك مع تشديد العقوبات

في حال تكرار اي فعل من هذه الافعال حسب المادة ١٠٨ على ان لا تجري الملاحقة حسب المادة ١٠٩ الا بناء على شكوى المتضرر.

ثانيا: في مطابقة قانون المعاملات الالكترونية وحماية البيانات الشخصية للمعايير الدولية

اذا ما استندنا الى المبادئ الدوليةوالاطر القانونية العامة التي استعرضناها سابقا نستخلص مجموعة شروط يجب توافرها في اي منظومة قانونية محلية لاسيما لجهة كيفية التعامل مع البيانات الشخصية والحقوق المترتبة لاصحاب البيانات ووجوب توافر عنصر الرضى وموجبات المسؤولين عن معالجة البيانات ووجود هيئة مشرفة مستقلة.

سنحاول تحليل الاطار القانوني الذي وضعه مؤخرا المشرع اللبناني في قانون المعاملات الالكترونية وحماية البيانات الشخصية ومدى انسجامه مع هذه المبادئ التي ذكرناها.

لعل ابرز الثغرات في القانون اللبناني بحسب القاضية هانية حلوة التي شاركت عن كثب في نقاشات مسودات القانون وبحسب ما استعرضته في جلسة نظمتها مؤسسة مهارات ومنظمة سمكس ضمن منتدى حوكمة الانترنت اللبناني في ٢٤ تموز الماضي عام ٢٠٢٠، بعنوان "التتبع الإلكتروني والشفافية لإدارة البيانات بمسؤولية"[59]؛ تطرقت من خلالها الى الأطر القانونية اللبنانية التي ترعى موضوع حماية البيانات وتوافقها مع المعايير الدولية. وشرحت القاضية حلوة أبرز الثغرات في قانون المعاملات الالكترونية وحماية البيانات الشخصية مؤكدة انّ "على الدولة اللبنانية أن تكون خاضعة لموجبات قوانين حماية البيانات الشخصية" وهذا الامر غير موجود في القانون كذلك ليس هناك اشارة الى موضوع الرضى وهناك ضرورة لوجود هيئة ناظمة مستقلة للرقابة المسبقة على حماية البيانات لأنّ الرقابة اللاحقة للحماية لا تكفي. ولفتت حلوة إلى أنّ "هذه الهيئة التي لم يتضمنها القانون بسبب تباين وجهات النظر السياسية هي أكثر من ضرورية

---

[59]ملخص جلسة "تطبيقات التتبع الالكتروني والشفافية لادارة البيانات بمسؤولية"، نظمتها مؤسسة مهارات ومنظمة سمكس، ٢٤ تموز ٢٠٢٠، http://maharatfoundation.org/igflebanon24july

وفق كل معايير الحماية". وخلصت الجلسة الى توصيات لتعديل قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي لجهة إضافة نص صريح بعدم أخذ أي بيانات شخصية من دون موافقة المستخدم المسبقة وبان يشمل تطبيقه الادارات العامة فضلا عن إضافة مواد إلى القانون المذكور تتعلق بالتجاوزات المتعلقة بخرق البيانات Data Breaching، وأصولها، وكيف نعترض عليها، ووجوب إنشاء هيئة ناظمة مستقلة تتيح الملاحقة المسبقة لضمان حماية البيانات وإيجاد آلية واضحة للتعامل مع خرق البيانات، واضافة نص يتعلق بأطر نقل البيانات وتبادلها داخل لبنان وخارجه (Data Transfer) وتأمين الحماية اللازمة لهذه البيانات خلال نقلها وتخزينها، والاهم ان تتم اضافة بنود واضحة حول ضرورة أن يكون السبب المشروع الذي يتيح جمع البيانات محدداً على عكس واقع القانون الحالي الذي لا يحّدد الغرض من جمع البيانات.

اذا يأتي هذا القانون ناقصا لجهة تطبيقه فقط على الشركات الخاصة التي تحتاج الى ترخيص لمعالجة البيانات كما نصت عليه المادة ٩٥ التي توجب من يرغب بجمع البيانات ومعالجتها اعلام وزارة الاقتصاد والتجارة بموجب تصريح نصت على تفاصيله التي اسلفناها المادة ٩٦. الا ان المادة ٩٤ أعفت حالات عديدة من التقدم بهذا التصريح وضمنها المعالجات التي يجريها اشخاص الحق العام كل في نطاق صلاحياته فضلا عن حالات اخرى استثنت الجمعيات والنقابات واصحاب المهن الحرة والمؤسسات التربوية وغيرها.

ان هذه الاعفاءات من التصريح تزيل عن القانون هدفا اساسيا ينشأ من اجله لحماية خصوصية الافراد وبياناتهم الشخصية إزاء تنامي جمع ومعالجة المعلومات من الادارات العامة مع المكننة والانتقال الرقمي. وهذا يتعارض مع المبادئ الدولية وإرشادات الاتحاد الاوروبي التي تخضع الادارات العامة مثل الشركات الخاصة الى موجبات لضمان حماية بيانات الافراد الشخصية.

كما ان قواعد جمع البيانات في المادة ٨٧ غير مفصلة لجهة تعريف الاهداف المشروعة التي ترعى جمع ومعالجة البيانات. تربط المبادئ العامة والمادة ٦ من إرشادات الاتحاد الاوروبي مشروعية الهدف بمعرفة ورضى صاحب البيانات الشخصية. هذا الشرط الاساسي المفروض في المعايير الدولية والذي يوجب تبليغ

صاحب البيانات اذا ما تغير الهدف من جمعها ومعالجتها في اي وقت لاستحصال موافقة ورضى جديد، لا نجده صواحة في القانون اللبناني المذكور، بل هناك ذكر عوضي لموضوع مشروعية الاهداف في المادة ٨٧ "على ان لا تتجاوز الاهداف المعلنة" وان يتم جمعها "بامانةولاهداف مشروعة ومحددة وصريحة" دون ذكر هذه الاهداف ودون ربطها بعنصر الوضى. هذا الوضى ايضا مذكور بطويقة عوضية في المادة ٤٩١ التي تتيح جمع البيانات الشخصية التي تكشف الحالة الصحية او الهوية الوراثية او الحياة الجنسي اذا وافق الشخص المعني صواحة على معالجتها. كما منعت المادة ٩٢ الشخص الطبيعي الاعتواض ولو لاسباب مشروعة اذا كان قد وافق على معالجة البيانات الخاصة به، وذلك بالوغم من ان المعايير الدولية تجيز سحب الوضى في اي وقت. وايضا المادة ٩٤ (٧) اعفت التقدم باي تصويح لمعالجة البيانات اذا وافق الشخص مسبقا على معالجة بياناته.

ويكون بذلك المشوع اللبناني قد غفل عن جعل الوضى والهدف المشروع اساسا لمعالجة البيانات ما يتعارض مع المبادئ الدولية.

كما ان التقدم بالتصويح الى وزارة الاقتصاد والتجارة وجعلها الجهة المولجة في موضوع التعامل مع طلبات معالجة البيانات لا يتوافق مع ضرورة وجود هيئة مستقلة عن السلطة السياسية تعنى بحماية البيانات وتقدم اليها طلبات الوصول والتصحيح وغوها من الممارسات الناتجة عن الحقوق المترتبة لاصحاب البيانات. كما يسمح القانون لوزارات اخرى الاشواف على عملية معالجة البيانات منها وزارتي الداخلية والدفاع في المادة ٩٧ فيما يتعلق بالامن الخارجي والداخلي للدولة. هذا المصطلح الفضفاض نراه ايضا في المادة ١٠٣ التي تمنع صاحب البيانات من الاطلاع عليها اذا كان ذلك يعوض غاياتها أو أمن الدولة الداخلي أو الخارجي للخطر. كذلك تعطي المادة ٩٧ الصلاحية لوزارة العدل بإعطاء التراخيص للبيانات المتعلقة بالدعاوى القضائية بمختلف أنواعها، وتعطي وزارة الصحة الصلاحية باتخاذ الإجراءات في الحالات الصحية أو بالهوية الجينية أو بالحياة الجنسية للأشخاص. كل ذلك يتعارض طبعا مع ضرورة تكليف جهة

مستقلة عن السلطة السياسية للاشراف على حماية البيانات منعا للتواطؤ بين الشركات الخاصة التي قد تكون لديها علاقات جيدة او مصالح مع الوزارات المعنية.

اما بالنسبة لمسؤولي معالجة البيانات فليس هناك اية تفاصيل حول كيفية تعيينهم والاخلاقيات الواجب عليهم الالتزام بها على عكس المادة ٤٠ من ارشادات الاتحاد الاوروبي التي تنص على التقيد بمدونات سلوك. كما ان ليس هناك مواد تتعلق بواجب هؤلاء المسؤولين عن البيانات بابلاغ اصحابها عن خروقات بياناتهم. هذا فضلا عن اعطائهم حق رفض حق الوصول والتصحيح اذا وجدوا الطلب متعسفا ما يعتبر تضييقا للحق.

المبحث الثالث: التعامل مع البيانات الشخصية في الواقع اللبناني

بعد ان استعرضنا المنظومة القانونية اللبنانية التي ترعى ضمان حماية البيانات الشخصية، من المهم ان نلقي الضوء على كيفية تعاطي الادارة اللبنانية والقضاء مع موضوع حماية البيانات الشخصية للوقوف على ما اذا كان يشكل اولوية ولو كان ذلك في اطار القوانين الموجودة اصلا والواجب النظر فيما اذا كان تطبيقها يتم بمراعاة المعايير الاساسية لحماية حق المواطنين بخصوصية بياناتهم الشخصية.

لذا سنقوم باستعراض حالتين متعلقتين بالتعامل مع موضوع معالجة البيانات الشخصية. الحالة الاولى تتعلق بوزارة الاتصالات وتسليمها كافة البيانات الخاصة بالاتصالات لكل المواطنين اللبنانيين الى الاجهزة الامنية لما اخذه هذا الموضوع من مساحة نقاش في الحيز العام، والحالة الثانية مبادرة خاصة لمجموعة لديها موقع الكتروني تجمع فيه بيانات تتعلق بالسجل التجاري بهدف ربط شبكات المصالح، وتم حجب الموقع بحجة انتهاك البيانات الشخصية. وبذلك نكون قد استعرضنا تعاطي ادارة عامة مع موضوع البيانات ومبادرة مجموعة خاصة تنشر بيانات اعتبر بعضه شخصيا يستوجب الحماية بموجب قرار قضائي.

المطلب الاول: انتهاك خصوصية البيانات الشخصية في ما يعرف بـ "داتا الاتصالات"

ابتداء من تموز عام ٢٠١٢، سلمت الحكومة اللبنانية كافة البيانات الخاصة بالاتصالات في لبنان للأجهزة الأمنية، وقد وافق مجلس الوزراء على تسليمها رغم وجود جدل حول هذه الخطوة واعتراضات من قبل المواطنين والناشطين وبعض التيارات السياسية، وهو ما يعد انتهاكا لخصوصية المواطنين اللبنانيين. مدد مجلس الوزراء في ١١ ايلول ٢٠١٤ مهلة تسليم الداتا كاملة لغاية ٣٠ نيسان ٢٠١٦ [60]، وطلب الى وزير الاتصالات اتخاذ التدابير الفورية اللازمة لتأمين حركة الاتصالات كاملة للاجهزة الامنية [61].

هذا في وقت لم تعطِ المادة ٩ لرئيس مجلس الوزراء أو لمجلس الوزراء الصلاحية المطلقة في مراقبة اتصالات جميع المواطنين، بل قيد المشرع هذه العملية، حماية للمبادئ الدستورية، ولكي يكون القرار قانونياً وجب أن يحدد في متنه الوسيلة والمعلومة والمدّة، على أن لا تتجاوز الشهرين اللذين تتم فيها عملية الاعتراض، وهذا الأمر لم تتم مراعاته.

وكان قد سبق ان تم تكليف رئيس مجلس الشورى شكري صادر مع وفد مرافق (المقدم انطوان قهوجي، الرائد المهندس خالد يوسف، العميد المتقاعد جوزيف نصار) زيارة الى فرنسا للاطلاع على الاطر القانونية لمراقبة حركة الاتصالات في الدولة الفرنسية وذلك عام ٢٠١٢.

وقد نشرت جريدة الجمهورية تفاصيل التقرير الذي تم تقديمه الى مجلس الوزراء في حينه [62].

---

[60] مقررات جلسة مجلس الوزراء في 29 نيسان 2015، وضمنها الموافقة على تمديد العمل بقرار مجلس الوزراء رقم 68 تاريخ 11/9/2014 المتعلق بتمديد مهلة إعطاء حركة الإتصالات كاملة للأجهزة الأمنية والعسكرية وذلك لمدة سنة تنتهي بتاريخ 30/4/2016 http://www.pcm.gov.lb/arabic/subpg.aspx?pageid=6959

[61] تقرير حرية الانترنت، مؤسسة مهارات، ٢٠١٥، ص ٤٢، http://maharatfoundation.org/media/1639/حرية-الانترنت-في-لبنان.pdf والتقرير المحدث المنشور في ٢٠١٨ http://maharatfoundation.org/internetfreedom2018

[62] https://www.aljoumhouria.com/ar/news/33548/الجمهورية-تنشر-تقرير-لجنة-التنصت-المعدل-في-فرنسا

وقد جاء في التقرير ان احكام القانون اللبناني رقم ١٤٠ مستوحاة بشكل كبير من احكام القانون الفرنسي الرقم 646-91 تاريخ 10/7/1991 والمتعلق بسرية المخابرات الجارية بواسطة وسائل الاتصال الالكترونية، لا بل ان الفصول المتعلقة بآلية اعتراض المخابرات كما وبإنشاء الهيئة المستقلة المنوط بها التثبت من قانونية اجراءات الاعتراض الاداري على المخابرات الهاتفية في القانون اللبناني هي شبيهة الى حد كبير بتلك الواردة في احكام القانون الفرنسي. بالفعل، واستنادا الى احكام القانون اللبناني والفرنسي المذكورين اعلاه، فإنّ الآلية المعتمدة للاعتراض الاداري تتلخص بما يلي:

وفق القانون اللبناني:

- يجيز وزير الداخلية او وزير الدفاع الاعتراض الاداري بقرار خطي معلل.
- لا يصبح قرار الاعتراض المتخذ من وزير الداخلية او وزير الدفاع نافذا الّا بعد موافقة رئيس مجلس الوزراء.
- ان رقابة الهيئة المُناط بها التثبت من قانونية الاجراءات المتعلقة باعتراض المخابرات بناء على قرار اداري هي رقابة مؤخرة واستشارية

ووفق القانون الفرنسي:

- يتقدم وزير الداخلية او وزير الدفاع او وزير المالية باقتراح قرار معلل بالاعتراض الاداري.
- يصدر رئيس مجلس الوزراء قرار الاعتراض الاداري بموجب قرار معلل (المادة ٤)
- ان رقابة الهيئة المناط بها التثبت من قانونية الاجراءات المتعلقة باعتراض المخابرات بناء على قرار اداري هي رقابة مؤخرة واستشارية (المواد 13و 14من القانون رقم 646-91تاريخ 10/7/1991).

وقد شرح التقرير ان الهيئة المستقلة المناط بها الرقابة على قانونية الاعتراضات الادارية تتمتع بسلطة رقابة استشارية ومؤخرة وانه سواء في القانون الفرنسي او القانون اللبناني فإن السلطة صاحبة الاختصاص والصلاحية بشكل مطلق لإعطاء الاذن بالاعتراض الاداري او عدمه تبقى مناطة برئيس الحكومة شخصيا

الذي يتمتع بسلطة مطلقة Pouvoir Regalien بهذا الشأن كونه يمثل الجهاز المناط به وضع السياسة العامة للبلاد والسهر على حسن تنفيذ القوانين بما يتوافق مع مصلحة الدولة العليا.

واشار التقرير انه وخلافًا لاحكام القانون الفرنسي (المادة ١٤من قانون ١٩٩١) فإن عرفًا اتبع في فرنسا يحيل بموجبه رئيس مجلس الوزراء اقتراحات الوزراء (دفاع، داخلية، ومالية) بالاعتراض الاداري الى الهيئة المستقلة المكلفة مراقبة قانونية الاعتراضات لاستشارتها، وذلك قبل ان يتخذ قراره بالموافقة على الاعتراض اورفضه. كما تجدر الاشارة ايضا الى ان اقتراحات الاعتراض من قبل الوزراء المختصين في فرنسا يجب ان تكون معللة وفقًا للاسباب التي تبرر الاعتراض والمنصوص عليها حصرا في المادة الثالثة من القانون 646/1991 وهي:

- الامن القومي.
- مكافحة الجريمة المنظمة.
- مكافحة التجسس الاقتصادي والصناعي والعلمي.
- اعادة تنظيم جمعيات تم حلها لمخالفتها الانتظام العام.

واستخلص التقرير مجموعة نقاط مهمة هي:

- اجمعت الاجهزة الامنية والقضائية في فرنسا على اعتبار ان كل طلب يرمي الى اعتراض مخابرات هاتفية (اي التنصت) يجب ان يكون معللا ومحصورا ان من حيث الارقام المنوي اعتراض مخابراتها او من حيث الاشخاص اصحاب تلك الارقام وهذا يشبه ما هو معمول به في لبنان.
- اجمعت ايضا تلك الاجهزة على اعتبار ان حركة الاتصالات الهاتفية الشاملة والذي يقابله في فرنسا ما يسمى باستثمار المعطيات التقنية للاتصالات Exploitation des données Techniques de Telecommunications والتي تشكل احدى مكوناته الفواتير الهاتفية المفصلة Facturation Détaillée شأنها تماما شأن طلبات اعتراض المخابرات، فلا تعطى الا بناء لطلب محصور ومعلل

يحدد فيه اسماء او ارقام المشتبه بهم كما ونوع الجرم المنوي اسناده اليهم، على ان تكون هذه الطلبات متناسبة مع نوع الجرم وان تكون الغاية من ورائها واضحة. كما اجمعت ايضا على ان تسليم حركة الاتصالات بشكل كامل وشامل من اجل ما يسمى "البحث الشامل "او Data Mining الى الاجهزة الامنية تتعارض مع احكام القوانين المرعية الاجراء في فرنسا.

- تمت الاشارة في بعض اللقاءات الى ان عدد المستخدمين على شبكات الهاتف الخلوي يتزايد باستمرار اذ يبلغ عدد المستخدمين حاليا في فرنسا حوالى ٦٠ مليون مستخدم، مما يشكل صعوبة في تخزين ومعالجة الحجم الهائل لحركة الاتصالات التي تنتج عن هؤلاء المستخدمين، هذا على فرض ان القانون الفرنسي يجيز تلك العملية.

- تبين من خلال اللقاءات ان للهيئة المستقلة الحق بالطلب الى الاجهزة الامنية اطلاعها على نتيجة اعتراض مخابرات اعطي الترخيص الاداري بالقيام بها وما اذا كان الاعتراض قد ادى الى الغاية التي من اجلها اعطي الترخيص.

- كما تبين ايضا ان هناك شركات اوروبية تعمد على تجهيز بعض البلدان ببرامج وتجهيزات اعتراض شاملة للمخابرات مبررة ذلك بأن قوانين تلك البلدان تسمح بذلك بالرغم من ان قوانين البلدان التي تنتمي اليها تلك الشركات لا تسمح بمثل تلك الاعتراضات.

- اخيرا،واثناء اجتماع الوفد اللبناني بالقضاة المولجين اعطاء الاذن القضائي باعتراض المخابرات وبالقضاة المختصين بجرائم الارهاب، تم عرض للواقع اللبناني الامني في ظل الظروف الصعبة والاستثنائية التي تمر بها المنطقة المحيطة بلبنان، كما تم استعراض الوسائل التي قد تسمح للاجهزة الامنية القيام بالحماية الوقائية من العمليات الارهابية المحتملة، كما وحماية المواطن من الجريمة المنظمة والجرائم الخطرة، وقد لمسنا من هؤلاء القضاة تفهماً لجهة امكانية تعديل المادة الاولى من القانون 140/99 بحيث يتم استثناء حركة الاتصالات الشاملة من نطاق احكامه لما تمثله من اهمية بالنسبة للاجهزة الامنية اللبنانية كونها

ساهمت وتساهم بشكل كبير في كشف الجرائم الارهابية وشبكات التجسس وغيرها من الجرائم الهامة. وقد تم اعلامنا ان اخراج حركة الاتصالات الشاملة من نطاق تطبيق احكام قانون حماية سرية التخابر لا يزال معمولا به في بعض البلدان العربية التي تعاني من اضطرابات داخلية وتهديدات امنية كما تبين ايضا انه في الولايات المتحدة الاميركية وعلى أثر الاعتداء الارهابي الذي حصل في 11ايلول 2001، اصدرت الحكومة الاميركية التشريع الشهير المعروف بالـ Patriot Act الذي سمح بموجبه للاجهزة الامنية بخرق بعض الحريات الاساسية (ومنها سرية التخابر) والقوانين السابقة المعمول بها، وذلك من اجل الكشف كما والوقاية من عمليات ارهابية محتملة.

المطلب الثاني: قضية ش.م.ل.: اسماء محامي الشركات التجارية من البيانات الشخصية

تقدمت نقابة المحامين باستدعاء الى قاضية الامور المستعجلة في بيروت هالا نجا طالبة شطب اسماء المحامين من على الموقع الالكتروني shinmimlam سواء على صفحاته الالكترونية وقاعدة البيانات العائدة له. وقد اعتبر القاضي ان المعلومات المنشورة بخصوص المحامين ليست معدة لاطلاع الجمهور ولا هي تدخل في عداد البيانات الواجب نشرها في السجل التجاري فيكون نشرها من قبيل التعدي على بيانات ذات طابع شخصي. ومن حق نقابة المحامين ان تطلب رفع التعدي عن حقوق المحامين المنتسبين اليها ومن بينها حقهم حماية بياناتهم. وقررت القاضية نجا في ١٦ حزيران ٢٠٢٠ ابلاغ جميع مزودي الانترنت بما فيها شركات الاتصال والمديرية العامة للاستثمار والصيانة حجب الموقع حتى حذف البيانات المتعلقة باسماء المحامين.

ان هذه القضية أثارت الكثير من الاختلافات لاسيما بين مفهوم حماية البيانات ذات الطابع الشخصي الذي استندت اليه القاضية ومفهوم السرية المهنية التي استند اليها نقيب المحامين.

ان الموقع المذكور يعرض معلومات موجودة اصلا في السجل التجاري ويقدمها بطريقة مبتكرة ان لناحية التصميم او لناحية سهولة البحث الامر غير المتوفر على الموقع الالكتروني للسجل التجاري. ويعرف

اصحاب الموقع عن انفسهم انهم مجموعة مبرمجين من لبنان وهم يعرضون نفس المعلومات الموجودة في السجل التجاري بهدف تعزيز الشفافية والوصول الى المعلومات. الموقع لا يقدم اي معلومات جديدة انما فقط ما هو منشور ومتاح في السجل التجاري لكنه يسهل عبر طريقة العرض البصرية ومحرك البحث التفاعلي اظهار الروابط بين مالكي الشركات والمساهمين فيها عبر البحث عن اسمائهم ما لا يتيحه السجل التجاري الذي يجيز البحث فقط عن اسماء الشركات. وقد ارتكز نقيب المحامين في ردوده على القضية [63] على المادة 26 من قانون التجارة، والمادة 87 من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي.

طرحت هذه القضية جدلا حول ما اذا كانت وكالة المحامين للشركات تعتبر من البيانات ذات الطابع الشخصي التي تستوجب حمايتها، لاسيما ان قرار القاضية نجا استند في حجب الوقع على ان اسماء المحامين من البيانات ذات الطابع الشخصي، دون ان يتطرق الى السرية المهنية. وفي مقابلة لجريدة الاخبار اعتبر المحامي غسان مخيبر ان ايماء المحامين ليست من البيانات الشخصية لعدة أسباب، "منها أن نشر اسم المحامي وتوكيله هما شرط ترخيص واستمرارية الشركة (كما تلزمها المادة 62 من قانون تنظيم مهنة المحاماة) وأمين السجل التجاري ملزم بالتحقق سنوياً من هذه المعلومة. كما أن المحاضر السنوية للجمعيات العمومية تتضمن توقيعي المحامي والمدقق المالي، وهي معلومات للنشر. ثم إن العلاقة بين المحامي ومستشاره القانوني ليست خاصة (في ما عدا المعلومات الخاصة الواجب كتمها)، وصفة المحامي ليست سرية، وخاصة أن الوكالة تبرز في المحاكمة العلنية، إضافة إلى أن أسرار المهنة لا تعني سوى الأفراد، بينما المعلومة المعلنة تخصّ شركة وعوضاً يذكر اسم محاميها." أما الأخطر بحسب مخيبر "فهو الاجتهاد القانوني لاعتبار اسم المحامي سراً من أسرار المهنة، هذا خطير جداً، ويفتح الباب لاعتبار اسم

---

[63] "حجب موقع »ش م ل«: وكالة المحامي »معلومات شخصيّة«؟"، تقرير في جريدة الاخبار منشور في ٣٠ تموز ٢٠٢٠ https://www.al-akhbar.com/Lebanon/292151/حجب-موقع-ش-م-ل-وكالة-المحامي-معلومات-شخصي-ة

مدقق المحاسبة معلومة شخصية،ولاحقًا أسماء المساهمين وأعضاء مجلس الإدارة... وعندها تنتفي قيمة السجل التجاري ووظيفته". كذلك اعتبرت المفكرة القانونية [64]ان قرار الحجب يناقض المادة ٢٢ من قانون التجارة التي تكرس مبدأ شفافية السجل التجاري اذ ان "سجلّ التجارة يمكّن الجمهور من جمع المعلومات الوافية عن كل المؤسسات التجارية التي تشغل في البلاد". ولم يتم التمييز ابدا بين البيانات الواجب نشرها كاسماء المساهمين وعنوان الشركة وبين بيانات اخرى كاسم المحامي. واذا ما اردنا الاستناد الى قانون المعاملات الالكترونية وحماية البيانات الشخصية فيمكن هنا تطبيق المادة ٩٤ الفقرة ٣ حيث "لا يتوجب التقدم بتصريح او ترخيص لمعالجة البيانات في المعالجات التي يكون موضوعها مسك سجلات مخصصة، بموجب أحكام قانونية أو تنظيمية، لإعلام الجمهور والتي يمكن أن يطلع عليها كل شخص أو أشخاص لهم مصلحة مشروعة". وهنا تنطبق هذه الفقرة على حالة موقع shinmimlam حيث الهدف من معالجة البيانات المتعلقة بالسجل التجاري هو اعلام الجمهور ويمكن ان يطلع عليها كل شخص له مصلحة مشروعة. كما ان المبالغة في اعتبار البيانات ذات طابع شخصي يؤدي الى التوسع في تفسير هذه البيانات وبالتالي بالحد من الوصول الى المعلومات اذ تدخل البيانات الشخصية ضمن الاستثناءات التي تعفي الادارة من اعطائها نشرها، ما يضيق تطبيق هذا القانون وادخال العديد من البيانات ضمن الاستثناءات ما يؤثر سلبا على شفافية الادارة العامة.

وبحسب المفكرة القانونية فان المعطيات الخاصة بالمحامي والتي تناولها القرار لا تتصل باي معطى متصل بحياته الخاصة انما فقط بمعطيات مهنية تتعلق بتعيينه كمحامي لشركة تجارية، لاسيما ان القانون التجاري يوجب تعيين محامي للشركات المساهمة ونشر ذلك في السجل التجاري ما يزيل اي طابع شخصي عن

[64] "نقابة محامي بيروت تضحي بالشفافية باسم "خصوصية" اعضائها"، مقال في موقع المفكرة القانونية منشور في ٢٨ تموز ٢٠٢٠ https://legal-agenda.com/article.php?id=7040

اسمه. كما ان هذا القرار يضر بالمصلحة العامة اذ يسمح بحجب معلومات مهمة للرأي العام تفضح شبكات مصالح سياسية تجارية وذلك تحت غطاء حماية خصوصية المحامين.

الخاتمة

يأخذ اليوم النقاش المتعلق بحماية الخصوصية والبيانات الشخصية حيزا كبيرا في العالم، وقد استعرضنا في هذه الدراسة الاهمية التي أولتها جهات دولية عديدة في السنوات الاخيرة الماضية، ضمنها الامم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الاوروبي والمنظمات الحقوقية، بهذا الموضوع لاسيما ان مفهوم الخصوصية قد تبلور من خلال التطور التكنولوجي والتحول الرقمي وازدياد الابتكار. كما ان مفهوم البيانات الشخصية اصبح مرتبطا بالبيانات الكبيرة للمستخدمين Big Data التي يتم تجميعها ومعالجتها ويقتضي وضع اطر لحمايتها ايا كان الطرف الذي يعالجها.

وقد وضعنا المعايير الدولية التي يجب ان تشكل اساسا للتشريعات الوطنية المحلية لضمان الحق في الخصوصية وحماية البيانات الشخصية.

في ضوء ذلك أجبنا على الاشكالية الاساسية التي طرحناها حول الاطار القانوني ومدى ضمانه للحق بالخصوصية وفي حماية البيانات الشخصية في لبنان وفق المعايير الدولية التي استعرضناها.

حيث بينا ان الحق في الخصوصية في لبنان يتمتع بضمانة دستورية لاسيما ان مقدمة الدستور اللبناني تضمن الحريات الشخصية وترسخ التزام لبنان بالمواثيق الدولية لاسيما الاعلان العالمي لحقوق الانسان والعهد الدولي الخاص بالحقوق المدنية والسياسية اللذان تضمنا مادة صريحة تضمن الحق بالخصوصية. واستعرضنا القوانين اللبنانية التي تحمي الاوجه المتعددة المرتبطة بالحق في الخصوصية لاسيما حماية حرمة المنزل المضمونة في الدستور وفي القوانين الجزائية. وكذلك بالنسبة لحماية سرية المراسلات والاتصالات عبر قانون الاتصالات رقم ١٤٠ الذي يضع أطرا واضحة تحمي اللبنانيين من التنصت ومن خرق اتصالاتهم. الا اننا بينا ايضا التجاوزات التي ترتكبها السلطات العامة ان بالممارسة او بسبب الفراغ التشريعي. هذه حالة انتهاك خصوصية المواطنين اثناء التحقيق عبر تفتيش حواسيبهم وهواتفهم ما ثبته حكم قضائي رائد قضى انه لا يجب الاخذ بالادلة الناتجة عن هذا التفتيش كونه جرى خلافا للاصول وانتهك

خصوصية الافراد الذي يتم التحقيق معهم. وذكرنا ان هاجس الخصوصية غائب عن الادارة العامة عند استخدامها للتكنولوجيا عارضين حالة تتعلق بتطوير تطبيقات للتتبع الالكتروني لمكافحة انتشار الكورونا كاجراء مرتبط بالصحة العامة. وألقينا الضوء على غياب الاطر الناظمة لعمل مزودي خدمات الانترنت الذين يمكن ان يخرقوا خصوصية مراسلات واتصالات المستخدمين في اي وقت دون اي حدود. هذا فضلا عن غياب الحماية لوجه اساسي من اوجه الخصوصية الذي يتم اخلاؤه اهمية كبرى من المقررين الخاصين لحماية الخصوصية والحريات الاساسية وهو الحق بالسرية عبر استخدام الهوية المغفلة على الانترنت، لاسميا في الانظمة التي لديها منحى لقمع الناشطين الذين يعبرون عن رأيهم على الانترنت وينتقدون الاشخاص العامين او اولئك الذين يعتبرون من الفئات المستضعفة.

ولان حق الخصوصية ليس مطلقا ويمكن ان يتداخل مع حقوق اخرى لاسيما الحق بالتعبير استعرضنا المبادئ العامة التي رسخها الاجتهاد الدولي في هذا الاطار لجهة اعلاء المصلحة العامة لتحقيق التوازن بين الحقين. هذا المبدأ وجدناه ايضا في الاجتهاد اللبناني رغم ندرة القضايا المطروحة امام القضاء اللبناني بهذا الخصوص.

ثم انتقلنا الى الاطر والتجارب الدولية الموجودة لحماية البيانات الشخصية لاسيما اللائحة العامة لحماية البيانات الشخصية التي اعتمدها الاتحاد الاوروبي ودخلت حيز التنفيذ في ايار ٢٠١٨. وبعد ان عرفنا بمفهوم البيانات الشخصية وشروط معالجتها مسترشدين باللائحة العامة الاوروبية واهمية ان تكون محدودة ولاهداف مشروعة مع موجب اعلام أصحابها واعطائهم حقوق عليها وحمايتها والقبول بالمساءلة، حددنا الحقوق المترتبة للافراد على بياناتهم الشخصية لاسيما حقهم بالوصول والتصحيح والنسيان والاعتراض والتعويض وشددنا على عنصر اساسي هو ضرورة توافر رضى صاحب البيانات. ثم انتقلنا الى موجبات الجهة المعالجة للبيانات من تعيين مسؤول لمعالجتها واعلام اصحاب البيانات والحفاظ عليها وحمايتها.

وعلى ضوء هذه المبادئ قمنا باستعراض القوانين اللبنانية التي تتعلق بحماية البيانات الشخصية لاسيما قانون الاتصالات الذي يوفر حماية لبيانات الاتصالات وبعض القوانين الاخرى مثل السرية المصرفية وقانون العقوبات وبعض قوانين تنظيم المهن التي تمنع الوصول الى بيانات شخصية مرتبطة بمواضيعها. وأولينا اهمية خاصة لقانوني الوصول الى المعلومات الصادر في ٢٠١٧ وقانون المعاملات الالكترونية وحماية البيانات الشخصية الصادر في ٢٠١٨. يوفر قانون الوصول الى المعلومات حماية للبيانات التي تعالجها الادارات العامة وهي ذات طابع شخصي عبر منع نشرها والوصول اليها. ويشكل بذلك اطارا عاما اوليا لمبدأ حماية البيانات الشخصية المتواجدة في حوزة الادارة اذ عرفها واعطى اصحابها حقوقا عليها وفرض على الادارة مراعاة حمايتها وعدم الكشف عنها. ولكن يبقى هذا الاطار عاما لا يؤمن حماية فعالة للبيانات الشخصية بحسب المعايير الدولية التي ذكرناها سابقا لاسيما لجهة نقص تفاصيل آلية الحماية وموجبات الادارة ورضى صاحب البيانات والهيئة المستقلة للاشراف على احترام الادارات لموجب حماية البيانات. اما بالنسبة لقانون المعاملات الالكترونية وحماية البيانات الشخصية، فقد أثبتنا ان فيه ثغرات عديدة ولا يتماشى مع المعايير الدولية. لقد أتى هذا القانون ناقصا لجهة تطبيقه فقط على الشركات الخاصة التي تحتاج الى ترخيص لمعالجة البيانات كما ان الاهداف المشروعة لجمع ومعالجة البيانات غير مفصلة بوضوح كذلك عنصر الرضى غائب تماما كغياب الهيئة المستقلة المشرفة على معالجة البيانات وامور اخرى تتعلق بخرق البيانات وبنقلها.

اذا أجبنا على الجزء الثاني من الاشكالية حول الآليات المتاحة لصون الحق بالخصوصية وحماية البيانات الشخصية، وبينا النقص الكبير في المنظومة القانونية الحمائية للبيانات الشخصية وعدم تلبية القانون الجديد النتائج المرجوة من حماية البيانات الشخصية واستعرضنا حالتان تتعلقان بكيفية تعامل الادارة العامة والقضاء مع موضوع حماية البيانات الشخصية. في حالة "داتا الاتصالات" سمحت وزارة الاتصالات ورئاسة مجلس الوزراء بتسليم كافة البيانات المتعلقة بالاتصالات لجميع اللبنانيين بالرغم من الاستشارة القضائية والمشورة

الفرنسية بان هذا الامر يعد انتهاكا لخصوصية بيانات اللبنانيين. اما في الحالة الثانية فقد ارتأينا الاضاءة عليها لتبيان تعاطي القضاء اللبناني مع موضوع البيانات الشخصية حيث اعتبر اسماء محامي الشركات يعد من البيانات الشخصية التي يقتضي حمايتها بالرغم من الاراء القانونية التي تتحدث عن عمومية هذه البيانات بحسب قوانين التجارة وعن المصلحة العامة التي من اجلها نشرت هذه الاسماء لتبيان الروابط بين الشركات والمساهمين والمحامين ما قد يكشف شبكات المصالح من اجل الصالح العام.

وبذلك نكون قد أحطنا في هذه الدراسة بموضوع لا يحظى بالكثير من الاهتمام في لبنان والمنطقة العربية على كافة المستويات ان من الجهات التشريعية او القطاع العام او القطاع الخاص وحتى من المواطنين انفسهم. ولا نجد الكثير من الاجتهاد القضائي في لبنان حول الموضوع بالرغم من كثافته على مستوى المحاكم الاوروبية والدولية. ونامل ان يتمكن لبنان الذي لطالما اعتبر رائدا في حماية الحريات الاساسية والتزامه بالمعايير الدولية لاسيما في مقدمة دستوره ان يرقى الى اصلاح القوانين الموجودة اليوم لاسيما قانون المعاملات الالكترونية وحماية البيانات الشخصية الذي بينا ان فيه ثغرات عديدة لا تجعله متماثلا مع المعايير الدولية. كما يقتضي اعلاء شأن المبادئ القانونية والمعايير الدولية على الشؤون السياسية الضيقة التي بينا من خلالها كيف تتخطى الادارة اللبنانية الاراء القضائية او كيف تغفل في تشريعها انشاء هيئة مستقلة مشرفة لحماية البيانات اذ ان مثل هذه الهيئات دائما تشهد تنازعات سياسية وتعطى السلطة التنفيذية صلاحيات رقابية تفرغ الرقابة من مضمونها وتشكل مساسا بالحوكمة الرشيدة حيث لا يمكن للسلطة السياسية ان تراقب نفسها. كما ان هذه الموضوع له ابعاد اخرى غير الابعاد القانونية والتي تتعلق بضرورة تعزيز شفافية الادارات العامة والاجهزة الامنية في استخدام التكنولوجيا وادوات المراقبة والتعقب وتحديث البنية التحتية للانترنت في لبنان لتكون اكثر متانة وقدرة على مواجهة تحديات الامن السيبراي وامكانية خرق البيانات، طبعا مع تفعيل الاطر الناظمة لعمل الشركات المزودة لخدمات الانترنت وكافة الشركات الخاصة. هذا فضلا عن تعزيز ثقافة الخصوصية على كافة المستويات وربما بدءا بالبرامج التربوية وبرامج

تمكين موظفي الادارة العامة. كما يقتضي التعاطي بجدية مع الانتهاكات التي تحصل والممارسات عبر مساءلة المسؤولين وايجاد آليات شكوى فعالة للتعويض على المتضررين لاسيما اعادة النظر بضرورة تشكيل هيئة مشرفة مستقلة لحماية البيانات.

آملين ان تكون هذه الدراسة قد بينت اهمية الحق بالخصوصية وضمان حماية البيانات الشخصية وضرورة ان يرتقي لبنان بقوانينه وممارساته الى حماية هذا الحق وفق المعايير الدولية وفق ما هو مكرس في دستورنا اللبناني.

المراجع والمصادر:

- فتوش، نقولا وبرتران، أندريه؛ **الحق في حرمة الحياة الخاصة، والحق في الصورة**، المنشورات الحقوقية صادر، ٢٠٠٤.

Mendel, Toby and others; **Global survey on Internet Privacy and** –
ion, UNESCO series on Internet Freedom, 2012. **ressFreedom of Exp**

– Castet-Renard, Celine et autres; **Protection des Données Personnelles: Se mettre en conformité d'ici le 25 Mai 2018**, Editions Législatives, 2017.

– Desgens-Pasanau, Guillaume; **La protection des données personnelles,** Lexis Nexis, 2e edition, 2016.

- Kurbalija, Jovan; **An introduction to Internet Governance,** DiploFoundation, 2016.

- Kleinwachter, Wolfgang and others; **Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s**, IGF Berlin, 2019.

– Mattatia, Fabrice; T**raitement des données personnelles**, Eyrolles, 2013.

– Turk, Alex; **La vie privée en peril – Des citoyens sous contrôle**, Odile Jacob, 2011.

–Roux (A.); **La protection de la vie privée dans les rapports entre l'Etat et les particuliers**, Coll. Droit public positif.,éd. Economica.1983.

– RIGAUX (F); **La protection de la vie privée et les autres liens de la personnalité**, Bibliothèque de la faculté de droit de l'Université de Louvain, L.G.D.J. 1990.

– BEIGNIER (B.); **La protection de la vie privée en Droits et libertés fondamentau**x (sous la direction de R. Cabrillac, M.A. Frison–Roche, Th. Revet), Paris, Dalloz, 4è. éd. 1997.

– RAVANAS (J.); **La protection des personnes contre la réalisation et la publication de leur image**, L.G.D.J., 1978.

– Bouhadana, Irène and others; **Transparency in the Open Government Era**, Les Editions IMODEV, 2015.

– Westin, Alan; **Privacy and Freedom,** Athenum, 1967

- Gavison, Ruth; **Privacy and the Limits of Law**, the Yale Law Journal Vol. 89: 421, 1980

– Davies, Simon; **Big Brother: Britain's Web of Surveillance and the New Technological Order 23,** 1996

–"Privacy International" Organization, **A Guide for Policy Engagement on Data Protection, The Keys to Data Protection**, August 2018,

(https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf)

التقارير:

- تقارير "المفوضية العليا لحقوق الانسان في الامم المتحدة" حول الخصوصية على موقعها الالكتروني، https://www.ohchr.org، تاريخ الزيارة تموز وآب ٢٠١٩

- تقارير "منظمة الخصوصية الدولية" على موقعها: https://privacyinternational.org، تاريخ الزيارة تموز وآب ٢٠١٩

- مجلة "مهارات ماغازين" الصادرة عن "مؤسسة مهارات"، العدد الثالث حول الخصوصية، حزيران ٢٠٢٠، http://magazine.maharat-news.com/home?issue=3

- تقرير "حرية الانترنت"، "مؤسسة مهارات"، ٢٠١٥، http://maharatfoundation.org/media/1639/حرية-الانترنت-في-لبنان.pdf والتقرير المحدث المنشور في ٢٠١٨ http://maharatfoundation.org/internetfreedom2018

- "مؤسسة مهارات"، "قانون الحق في الوصول الى المعلومات: دراسة تقييمية عن تطبيقه واستخداماته"،، نشرت في شباط ٢٠٢٠ http://maharatfoundation.org/media/1783/access-study-2020.pdf

- التقرير الدوري الشامل حول حق الخصوصية في لبنان مقدم من منظمة تبادل الاعلام الاجتماعي، "سمكس" و"الخصوصية الدولية" و"جمعية الاتصالات التقدمية" الى مجلس حقوق الانسان، ٢٠١٥، https://www.upr-lebanon.org/wp-content/uploads/2015/11/289002529.pdf

- ورقة "بين احترام الحريات الشخصية ومراعاة مصلحة الدولة والأمن الوطني"، اعداد الدكتور نادر عبد العزيز شافي، دكتوراه دولة في الحقوق محام بالإستئناف، منشورة على موقع الجيش اللبناني، ايار

٢٠٠٧، https://www.lebarmy.gov.lb/ar/content/بين-احترام-الحريات-الشخصية-ومراعاة-مصلحة-الدولة-والأمن-الوطني

- مبادئ Necessary and Proportionate، طورتها مجموعة منظمات حقوقية دولية، ٢٠١٤، https://necessaryandproportionate.org/files/en_principles_2014.pdf

- منظمة Article 19، تقرير المبادئ العامة حول حرية التعبير والخصوصية، ٢٠١٧، http://article19.shorthand.com

- اطار الخصوصية الذي وضعته "منظمة التعاون الاقتصادي والتنمية"/ The OECD Privacy Framework، ٢٠١٣، http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

- Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 2010, https://www.echr.coe.int/Documents/Convention_ENG.pdf

- Britz, J.J.; Technology as a Threat to Privacy: Ethical Challenges to the Information Profession, paper issued by Department of Information Science,University of Pretoria, 0002 Pretoria, South Africa, 2014

المقالات:

- مقالات قانونية على موقع المفكرة القانونية الالكتروني: https://www.legal-agenda.com

- تحقيق في جريدة الاخبار، "انتهى ملف التنصت دون التطرق الى...التنصت، حسن عليق، ٤ شباط ٢٠٠٩، https://al-akhbar.com/Politics/143787

- "حجب موقع »ش م ل«: وكالة المحامي »معلومات شخصيّة«؟"، تقرير في جريدة الاخبار منشور في ٣٠ تموز ٢٠٢٠ https://www.al-akhbar.com/Lebanon/292151/حجب-موقع-ش-م-ل-وكالة-المحامي-معلومات-شخصي-ة

- تحقيق في جريدة الجمهورية، "الجمهورية تنشر تقرير لجنة التنصت المعدل في فرنسا"، منشور في ٢ تشرين الاول ٢٠١٢، https://www.aljoumhouria.com/ar/news/33548/الجمهورية-تنشر-تقرير-لجنة-التنصت-المعدل-في-فرنسا

القوانين:

- القوانين اللبنانية على موقع: http://www.legallaw.ul.edu.lb
- نص إرشادات الاتحاد الاوروبي لحماية البيانات الشخصية GDPR، https://eur-lex.europa.eu/eli/reg/2016/679/oj
- موقع الهيئة الوطنية الفرنسية لحماية حرية المعلومات، https://www.cnil.fr
- قرار المجلس الدستوري ٢/٩٩، http://www.cc.gov.lb/ar/node/2577
- https://www.aljoumhouria.com/ar/news/33548/الجمهورية-تنشر-تقرير-لجنة-التنصت-المعدل-في-فرنسا
- تفسير الحق في النسيان وفق موقع إرشادات الاتحاد الاوروبي لحماية البيانات الشخصية: https://gdpr.eu/right-to-be-forgotten/?cn-reloaded=1&cn-reloaded=1
- خلاصة حكم المحكمة الاوروبية في قضية غوغل ضد اسبانيا: https://epic.org/privacy/right-to-be-forgotten/

فهرست: